2009

The fair information principles: a comparison of U.S. and Canadian Privacy Policy as applied to the private sector

Shane Crounse

The Fair Information Principles: A Comparison of U.S. and Canadian Privacy Policy as Applied to the Private Sector

by Shane Crounse

Masters of Science
Science, Technology and Public Policy
Thesis Submitted in Fulfillment of the
Graduation Requirements for the

College of Liberal Arts/Public Policy Program at
ROCHESTER INSTITUTE OF TECHNOLOGY
Rochester, New York

January 2009

Submitted by:

Shane Crounse Date

Accepted by:

Dr. Franz A. Foltz, Thesis Advisor Date
Graduate Coordinator, STS/Public Policy Department
College of Liberal Arts

Dr. Samuel C. McQuade, Committee Member Date
Professor, Center for Multidisciplinary Studies
College of Applied Science and Technology

Dr. James J. Winebrake, Committee Member Date
Chair, STS/Public Policy Department
College of Liberal Arts

The Fair Information Principles: a Comparison of U.S. and Canadian Privacy Policy as Applied to the Private Sector

Abstract

U.S. consumers are worried about their privacy and their personal information. High profile cases of identity theft involving companies losing the private information of hundreds of thousands of customers have only served to elevate the mistrust consumers have for companies that collect and share their personal information. The Federal Trade Commission (FTC) is charged with protecting U.S. consumers from fraud, deception, and unfair business practices in the marketplace; a task made difficult by an overarching need to balance the rights of the individuals against the security needs of the country and the free flow of information required by a free market economy.

The FTC has asked U.S. companies to follow the Fair Information Practices developed by the U.S. government in 1973, but does not require adherence to those standards. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) was passed in 2000 to address the similar privacy concerns of their consumers. PIPEDA is based on the Fair Information Principles and requires that companies implement those principles.

The Privacy Policy Rating System (PPRS) has been developed for this thesis as a method of rating company privacy policies for how they compare to the Fair Information Principles. Using both the PPRS content analysis technique and a standard stakeholder analysis technique, company privacy policies in both countries are examined to address the question of which government's privacy policy is doing a better job of achieving the Fair Information Principles. The lessons learned in this comparison are used to formulate policy recommendations to improve U.S. privacy policy for better adherence among U.S. companies to the Fair Information Principles.

Table of Contents

Chapter 1: Background and Introduction

In his seminal work on the subject, Westin defined privacy as, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin, 1967, p._6)." It is this type of privacy that Westin claims has been around for as long as humans have grouped together. Specifically, Westin claims the concept of limiting the power of authorities to delve into individuals' affairs as something born out of early western societies such as the Greeks (Westin, 1967, p._7).

The United States Constitution does not specifically mention a right to privacy; however, the First, Fourth, Fifth, and Ninth Amendments all, to varying degrees, protect the basic right to privacy and against unwarranted search or seizure of personal affects and property. The U.S. Supreme Court has also defended the right to privacy in several important court cases. For example, in Katz v United States (1967), the Supreme Court ruled that government wiretapping of a phone booth conversation can constitute a violation of the Fourth Amendment. Silverman v United States (1961) found that illegal seizure extends beyond physical belongings to oral conversations, thus requiring law enforcement to get a warrant prior to observing private conversations. These and other cases outline the rights of citizens to be free from privacy violations by their government.

In their definitive work titled, "Right to Privacy," Warren and Brandeis claim that the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. (Warren & Brandeis, 1890)

It was Warren and Brandeis' idea that the existing laws and judgments have established a protection of person and property, but that the definition of person and property must be re-defined to incorporate societal changes. The authors claim in the past, conflicts have been defined as property rights or breaches of contract, but there is a right that does not fit neatly into one of these categories. They describe the right as, "to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others" (Warren & Brandeis, 1890). Warren and Brandeis wrote "Right to Privacy" in 1890, long before the Internet age or the creation of the automated personal data systems that would later inspire new definitions of person and property.

Privacy is critical to a free democratic society. When individuals lose the ability to develop relationships with other people at their own pace and lose the ability to control personal information about themselves, their situation is counter to several of the principles outlined in the U.S. Constitution including but not limited to; the freedom of religion, the freedom to assemble peacefully, and the right to be secure in their person and effects. A society in which nothing is private is a society in which aspects of an individual's life are susceptible to coercion of different forms.

The need for personal privacy, like other fundamental rights, must always be weighed against the needs of society as a whole. For example the right to free speech does not permit individuals to yell "fire" in a crowded theater. The right to privacy is likewise not absolute. In the United States, a free-market economy requires a free flow of information that can challenge personal privacy. Banks must know a certain amount of information about a client before they provide a loan. While that client may prefer to

keep that information private, the bank cannot provide the loan without a certain degree of comfort afforded by the client's credit history. The third mitigating factor in this balancing act is national security. Since the events of September 11th, the United States government has been very concerned with security. Knowledge continues to be power and personal privacy can be a threat to security if not properly balanced against the needs of society to know what some individuals are doing.

Westin claimed the same human desire for privacy is coupled with an equally strong human desire to know and invade the privacy of others (Westin, 1967, p. 5). Those afflicted by this desire to threaten the privacy of others can be found in government, corporations, and among the public at large.

Seminal Privacy Cases

Court cases involving privacy issues range from Roe v Wade which argued the privacy of a woman's right to terminate her pregnancy to McCall v The Sherwood Inn which involved hotel peeping toms. A subset of these court cases examines the types of information a company or private organization can legally discover and keep about individuals, and some of the privacy issues that may arise.

In September 1989, Sibi Soroka filed a class action lawsuit against Dayton Hudson Corp, which owns Target retail stores. During a job interview Soroka was asked to complete an extensive psychological exam that asked detailed questions about his religious, sexual and political beliefs as well as other topics. Due to his need for the job, Soroka completed the exam despite his growing uneasiness and later consulted an attorney. Soroka's lawsuit contended that the store had violated his privacy by requiring

him to answer questions that revealed extensive personal information and that such information was not necessary to evaluate him for the position. Target would later settle the suit when it became clear that the California Supreme Court would rule in Soroka's favor. Target stores no longer administer the tests to potential employees (Alderman & Kennedy, 1995, p. 277).

In 1988, Congress passed the Employee Polygraph Protection Act (EPPA) after several publicized cases involving applicants being asked to submit to polygraphs as a condition of a job application. In the case of Long Beach City Employees Association v City of Long Beach California, the polygraph examiners manual was cited as containing the questions outlined in Figure 1A. The questions were determined by the California Supreme Court to be, "specifically designed to overcome…privacy by compelling communication of thoughts, sentiments, and emotions which the examinee may have chosen not to communicate" (Alderman & Kennedy, 1995, p. 292).

Figure 1A: Polygraph Questions used by Long Beach California

- Have you had any major operations in the past ten years?
- Have you ever suffered a nervous breakdown?
- Have you ever filed or collected workmen's compensation insurance from an on-the-job injury?
- Have you ever had an automobile accident while you were driving?
- Are you now or have you ever been a Communist sympathizer?
- Have you written any bad or insufficient checks in the past three years?

(Alderman & Kennedy, 1995, p. 292)

These cases exemplify the court's inclination to protect individual privacy rights against intrusion from companies and organizations that have little or no legitimate business purposes to collect such information. Most violations occurred in person, with the victim being asked directly to reveal information about themselves. With the growing

use of computer technology in the latter half of the 20th century, the need to inquire directly is being replaced by access to large automated data systems developed from the paper files already in existence. These systems house a variety of information about individuals and their personal and professional histories. With an automated system in place, the data is more readily available and easier to transfer. It becomes less likely that consumers will be aware of information changes or transfers that could potentially violate their wishes or legal rights.

During his tenure as U.S. Secretary of Health, Education and Welfare, Elliot L. Richardson commissioned a report on automated personal data systems growing in use among both government and private sectors in the U.S. The Secretary commissioned the report, "in response to growing concern about the harmful consequences that may result from uncontrolled application of computer and telecommunications technology to the collection, storage, and use of data about individual citizens." The Commission did not release their report until after Secretary Richardson's tenure ended, but the report was fully supported by his successor Secretary Casper Weinberger (HEW Report, 1973).

Secretary's Advisory Committee on Automated Personal Data Systems

On June 5, 1973, the Secretary's Advisory Committee on Automated Personal Data Systems submitted a report to the Secretary of Health Education and Welfare (HEW) entitled, Records, Computers and the Rights of Citizen. The report explored the new paradigm of automated personal data systems. Secretary Weinberger's foreword to the report speaks of new technologies that may have consequences for American society. It was this report that called for a, "Code of Fair Information Practices" that would be

enforced by law to protect the rights of Americans against the threats posed by an emerging data driven society (HEW Report, 1973).

Although the report was written in the early 1970s, the U.S. government was already aware of the new paradigm posed by the emergence of new data systems. Secretary Weinberger's foreword states "high-speed telecommunications networks are destined to become the principal medium for making, storing, and using records about people." The foreword further cautions that while these new system offer great benefits, such as faster service and convenience; there are often consequences of new technologies that will be forced upon society without warning. Specifically, this caution focused on the possibility that computer applications may be used to oversimplify complex problems and that the victims of this oversimplification will be disadvantaged citizens that are unable to correct errors or misconceptions based on the oversimplified data. The secretary concludes the foreword by demanding a hard look at the adequacy of current mechanisms for "guaranteeing citizens all the protections of due process in relation to the records we maintain about them" (HEW Report, 1973).

Weinberger and the HEW Report provide a new definition of the "person and property" discussed in the Bill of Rights and the Warren and Brandeis article. The HEW report and the accompanying Fair Information Principles state "privacy is considered to entail control by an individual over the uses made of information about him." The report recommends legislation protecting specific rights, entitled the "Code of Fair Information Practices" as summarized in Figure 1B:

Figure 1B: Summary of Code of Fair Information Practices

- There must be no personal data record keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

(Records, Computers and the Rights of Citizen, HEW, 1973)

The Fair Information Practices have since become the standard for privacy protection. In 1974, Congress passed the Privacy Act, which applied the Fair Information Practices to all federal agencies. Since the release of the HEW Report in 1973, there has not been any enforceable law or regulation that would hold the private sector to the same standard that the Privacy Act (1974) applied to federal agencies. Presently the charge of consumer protection in the marketplace rests with the Federal Trade Commission (FTC).

The Federal Trade Commission (FTC) and Privacy

Loss of personal privacy and personal data has become an externality of everyday business. Consumers provide personal information about themselves in business transactions as a point of convenience and as a requirement of modern trade mechanisms. Credit cards, online purchases, and cheaper services, are all provided by using ever-improving technology to organize and analyze personal information (O'Harrow, 2006). It is for this reason that privacy is a policy issue. Collection of personal information can

have a negative impact on consumer welfare, and this impact is not captured accurately in the marketplace (Hui, 2005). It is for this reason that the FTC is charged with consumer protection and has the ability to regulate the market of personal information collection and use.

According to the FTC website, the Commission is the "nation's consumer protection agency" (ftc.gov, 2007). The FTC is responsible for regulating the relationship between individuals and businesses or other private organizations. One of the FTC's stated goals is to, "Enhance consumer confidence by enforcing federal laws that protect consumers (ftc.gov, 2007)." The FTC's Division of Privacy and Identity Protection is its newest division and it oversees "issues related to consumer privacy, credit reporting, identity theft, and information security" (ftc.gov, 2007). This division is also responsible for enforcing a subset of laws that deal with consumer privacy. Figure 1C summarizes these responsibilities. The FTC is the U.S. government's representative in the privacy policy arena. This role places special attention on statements and reports issued by the FTC regarding their goals and objectives as they relate to privacy and the protection of personal information and the FTC's own report entitled Privacy Online: Fair Information Practices in the Electronic Marketplace, concluded that the current policy of industry self-regulation is not achieving the FTC's goals and requires change (2000). This thesis explores one avenue of possible change.

Figure 1C: FTC Division of Privacy and Identity Protection Responsibilities

Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, including deceptive statements and unfair practices involving the use or protection of consumers' personal information; The Fair Credit Reporting Act, which ensures the accuracy and privacy of information kept by credit bureaus and other consumer reporting agencies, and gives consumers the right to know what information these entities are distributing about them to creditors, insurance companies and employers; and The Gramm-Leach-Bliley Act, which requires financial institutions to ensure the security and confidentiality of customer information, provide notice to consumers about their information practices, and give consumers an opportunity to direct that their personal information not be shared with certain non-affiliated third parties (http://www.ftc.gov/privacy/privacyinitiatives/promises.html, 2007)

Technology and Privacy

Effective privacy policy must account for the constant evolution in technology and establish principles that will continue to be relevant regardless of technological progression. The continued evolution of data technology allows an ever-increasing amount of data to be transmitted quickly and cheaply around the world. That information can be accessed from and downloaded to hand-held devices, wirelessly connected to the Internet. U.S. consumers are able to surf the web for the answers to virtually any question they can conceive. Online business transactions have become the norm and most Americans have information about them stored somewhere in a database, whether it is their medical history, their purchasing habits, or other types of personal information.

Privacy has been a concern as long as human societies have existed. Technology continues to make the issue of safeguarding privacy more complex. The creation of automated personal data systems in the middle of the twentieth century was a defining

moment. This new technology made it possible to store electronic records about millions of individuals and access that information quicker and cheaper than in the past. In order to address the modern issues of privacy and personal information protection, it is necessary to consider the continuing evolution of technology and how it affects personal privacy.

Current Privacy Threats

Threats to privacy exist in every society, and in all countries. Consumers in the United States face continuous threats to their personal privacy. Personal privacy can be threatened by the actions of organizations as well as individuals. An individual may present a threat to privacy in several forms, such as stalking, harassment, or identity theft. Organizational threats can come from governmental organizations such as law enforcement, or private organizations such as companies.

Government organizations can threaten personal privacy in a variety of ways including domestic spying by intelligence agencies (Schmitt, 2007) and law enforcement profiling (Lichtblau, 2006). Less obvious but equally dangerous threats also come from the Social Security Administration, the Internal Revenue Service, and the Department of Veterans Affairs among others (Sorrell, 2005). These agencies all collect personal information about individuals in databases as part of their agency missions. These databases can be compromised by outsiders or even abused by agency employees who have intentions of hurting political enemies or even performing a background search on an attractive woman (O'Harrow, 2006 pg_274).

Private organizations also collect personal information about individuals for a variety of reasons, which is the focus of this thesis. Some companies, for example, maintain very large databases that contain as much purchasing information as can be collected about consumers in order to better target their marketing campaigns (McWilliams, 2004; Freed, 2004). Retailers such as Amazon.com or Buy.com, maintain customer databases containing shopping history and buying habits. Credit agencies Equifax, Experian, and Trans Union all maintain databases that are used by a variety of organizations, both governmental and private, for information about individual credit history. Internet Service Providers (ISPs) provide Internet access to millions of customers and maintain records of what those users do while they are online. Modern cell phones contain Global Positioning Systems (GPS) which allow the cell phone companies to monitor where and when phones are used. News reports as old as 2006 have claimed that law enforcement can even listen to conversations that occur near a cell phone, even while the phone is turned off (McCullagh, 2006).

The current situation in both the United States and Canada finds each of these threats to privacy addressed differently. Both countries have laws, the U.S. Privacy Act of 1974 and the Canadian Privacy Act of 1983, respectively that regulate government entities and reduce the threat they pose to personal privacy. Both countries also have laws that restrict the behavior of individuals and provide civil and criminal penalties for certain violations of personal privacy, including identity theft and stalking. In the United States, individual states have passed such laws rather than the federal government. In Canada it is the federal code that addresses cyber stalking (justice.gc.ca, 2003, and USDOJ 1999).

The major difference appears between how the United States and Canada handle threats to privacy posed by private organizations. The Canadian Parliament, in 2000, passed the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA is a law that regulates all private organizations that handle personal information. PIPEDA is designed to extend the extensive protections provided by the 1983 Privacy Act to include the private sector.

The United States Congress has implemented a more piece-meal approach to regulating companies. Congress has passed several privacy laws that apply only to certain industries, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 concerning the health care industry. Beyond HIPAA, Congress also passed the Fair Credit Reporting Act (1992), the Gramm-Leach-Bliley Act (1999), the Electronic Communications Privacy Act (1986), the Family and Educational Privacy Act (1974), the Video Privacy Protection Act (1988), the Telephone Customers Protection Act (1994), and the Drivers Privacy Protection Act (1994). There are also numerous state and local laws dealing with specific industries or aspects of personal privacy. This thesis will not examine the privacy policies of individual U.S. states or Canadian provinces. The focus will remain on national privacy policy and the results being achieved by those national policies.

The following chapters compare how the U.S. and Canada regulates private organizations and the threat they pose to personal privacy. The objective is to highlight the differences in each country's policies and their achievements thus far based on existing work conducted by other researchers.

Thesis Roadmap

Current U.S. privacy policy does not meet the goals outlined by the 1973 HEW report and the current FTC recommendations. The continuing literature review in Chapters 2 and 3 provide an analysis of the current state of privacy policy in the United States and Canada. Research questions are developed in Chapter 4 to provide a framework for exploration of the topic. Chapter 5 outlines the methodology chosen to answer the research questions. The methodology includes a description for choosing the particular data that is examined and how that data provides answers to the research questions posed in Chapter 4.

Chapter 6 outlines the analysis and discusses the results of the industry privacy policy analysis. Privacy policies from U.S. industries are compared to those of Canadian counterparts to determine which country is producing industry privacy policies more closely in line with the Fair Information Principles outlined in the 1973 HEW Report and the FTC guidelines. Chapter 7 provides context to the Chapter 6 comparison with an analysis of privacy policy stakeholders and their positions, goals and objectives for privacy policy. Stakeholders in both the United States and Canada will be examined to determine their role in policy development and their probable impact on the end result.

The data from Chapters 6 and 7 is synthesized and used to answer the research questions posed in Chapter 4. The results are outlined and discussed using case studies in Chapter 8. These results lead to several policy recommendations which are covered in Chapter 9. The policy recommendations are intended for U.S. policymakers, including representatives in Congress as well as those in the executive branch, particularly the FTC.

Chapter 10 discusses the limitations of content analysis and stakeholder analysis research design, the selected data sources, and methodology applied in conducting the research. Chapter 10 also includes recommendations for future research that could possibly provide additional insight into the challenges of U.S. privacy policy.

Chapter 2: The U.S. Situation

U.S. legislation and regulation governing privacy matters are targeted at specific government agencies, industries and business, or they are targeted as specific types of personal information or situations. On top of the federal rules, each state may have developed their own respective policies, which are more stringent than federal regulations. While this thesis does not include discussion of individual state rules, it is important to review some examples of targeted federal rules that demonstrate this fragmentation of privacy policy.

The Gramm-Leach-Bliley Act of 1999 focuses on financial institutions and their procedure for handling individual's financial information. The Act focuses on what financial institutions can and cannot do with an individual's financial information and what rights individuals have to control that information. Along similar lines, the Fair Credit Report Act of 1992 regulates the credit reporting industry and is also charged with protecting the confidence the U.S. economy puts in this industry. The Children's Online Privacy Protection Act of 1998 focuses on websites that collect information about the individuals who visit that site and what those sites must do to protect children from privacy violations or harmful situations.

There is no single piece of U.S. legislation or regulation that controls all personal information collected by all private organizations. Outside of the targeted laws and regulations, the official U.S. policy has been industry self-regulation. In May 2000, the U.S. Federal Trade Commission (FTC) released a report titled, "Privacy Online: Fair Information Practices in the Electronic Marketplace." The FTC report concluded the current policy of industry self regulation is failing to sufficiently enforce the Fair

Information Principles developed by the 1973 HEW Commission. The FTC report reiterates the importance of these privacy principles and recommends legislative action in order to establish a basic level of privacy protection (FTC, 2000).

History of Current U.S. Privacy Policy

The FTC is charged with protecting U.S. consumers and is charged with implementing several of the laws that affect U.S. consumer privacy, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and Children's Online Privacy Protection Act (ftc.gov, 2007). It is this mandate that makes the FTC the primary enforcer of consumer privacy legislation in the United States. In 1996 the FTC produced a report titled "Anticipating the 21st Century: Consumer Protection Policy In The New High-Tech, Global Marketplace." This report outlined the role the FTC believed it should play in protecting consumers affected by emerging information technologies. The report recognized the threat posed to privacy by new technologies, such as large databases and data mining software. Within the report, the authors weigh the arguments for and against legislating privacy protection. In the end, the FTC decided in favor of a "balanced consumer protection program" (Figure 2A).

Figure 2A: Summary of 1996 FTC Report Recommendations

- Coordinated law enforcement by state and federal agencies against fraud and deception;
- Industry self-regulation and private initiatives to protect consumers; and
- Consumer education through the combined efforts of government, business, and consumer groups.

(FTC, "Anticipating The 21st Century: Consumer Protection Policy In The New High-Tech, Global Marketplace" 1996)

Since the release of the 1996 report, the FTC has implemented these recommendations. Their website lists a number of high profile cases in which fraud and privacy laws have been enforced against companies and individuals. It would appear that their first goal of coordinated law enforcement is being achieved through litigation and administration of fines and penalties.

The FTC has also allowed industry to self-regulate privacy protection beyond specific pieces of legislation passed by Congress. Industry has established certifications, such as the TRUSTe symbol that is posted prominently on a websites privacy policy statement indicating adherence to a set of privacy standards (truste.org, 2007). This demonstrates an effort by industry to meet the second goal of the 1996 FTC report by creating standards and guidelines to protect consumers.

The FTC itself has followed a campaign of consumer and business education. Among other initiatives, their website provides multiple sources for both consumers and business to learn about privacy and the roles of all parties involved. There are consumer guides to protecting personal information and business guides that recommend best practices for both protecting consumer information and informing consumers of business practices (ftc.gov, 2007).

For individuals, there is a more extensive brochure that explains a variety of information ranging from credit scores and credit agencies to how to protect identity from criminals. The brochure is designed to educate consumers about a broader range of threats to consumers, aside from identity theft. These are examples of the educational initiatives described in the 1996 report. Unfortunately, the initiatives outlined in the 1996

report are not doing enough to address the concerns of the FTC, as stated in their more recent 2000 reports.

Evaluations of the Current Situation

In 2000, the FTC issued several reports regarding consumer privacy and the threats to privacy posed by data gathering conducted by private organizations. These reports concluded that the FTC's plan for industry self-regulation developed in 1996 is not achieving the desired outcomes and should be supplemented with federal regulation that provides a baseline of consumer protection. One such report titled, "Fair Information Practices in the Electronic Marketplace," was presented to Congress and told a story of progress, but not success. The FTC surveyed company websites to determine how companies have been following the government's Fair Information guidelines for informing consumers of their business practices. The survey found that while as many as ninety nine percent (99%) of websites surveyed collected personally identifiable information; only twenty percent (20%) had a posted statement that addressed, in part, the Fair Information Practice principles. While these numbers show improvement over previous surveys, the numbers are not satisfactory to the FTC (FTC, 2000).

The report also discusses the extent to which industry self-regulation has been adopted through the use of website privacy seals. These types of programs require organizations to meet certain minimum safeguards in order to receive a seal of approval from one of several private certification programs. The FTC survey found that only eight percent (8%) of websites surveyed displayed any privacy seal. While the report recognizes the efforts of industry and the success they have achieved thus far, the report

concludes that industry self-regulation is not sufficient to achieve the results the agency supports. The report recommends federal legislation as the best way to affectively attain the desired level of privacy protection. They recommend that consumer-oriented commercial websites which collect information about consumers be required to comply with the Fair Information Practices. Specifically, commercial websites would have to meet the following requirements outlined in Figure 2B.

Figure 2B: Fair Information Practices Recommendations by 2000 FTC Report

- **Notice:** Websites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (*e.g.*, directly or through non-obvious means such as internet cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
- **Choice:** Websites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (*e.g.*, to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).
- **Access:** Websites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.
- **Security:** Websites would be required to take reasonable steps to protect the security of the information they collect from consumers.

These requirements would be applicable only to sites that were commercially oriented and that did not already fall under other legislation requiring alternate levels of protection (ftc.gov, 2007). This applicability standard would seem to leave significant gaps in consumer protection. Other assessments recommend different actions.

Additional Assessments of Privacy Policy

The Federal Trade Commission is not the only organization that has been examining the condition of privacy protection in the U.S. Other organizations have issued reports describing their research on the subject and their recommendations for action. One such report was presented by faculty from the University of Pennsylvania at the Federal Trade Commission (FTC) meeting in November of 2006 (Turow, 2006).

The UPenn report examined other efforts to protect consumer privacy. The report describes the lack of awareness on the part of consumers regarding their privacy rights and their lack of awareness of the requirements placed on organizations that may be collecting their information. Their research demonstrated that consumers believe the term "privacy policy" displayed on a company website means that company meets a certain baseline for privacy protection, which is not accurate. The report concludes that a lack of baseline standards causes consumer confusion.

The UPenn report also sites a survey conducted by the Annenberg Public Policy Center at UPenn where seventy percent (70%) of respondents agreed or strongly agreed with the statement, "I am nervous about websites having information about me." Respondents also felt they were at risk as a result of companies collecting their information (Turow, 2003). Both conclusions, the confusion of consumers and their concern, corroborate the conclusions drawn by the FTC that their 1996 plan is not working and that a change in policy is necessary. The UPenn report also called for legislative or regulatory requirements that would establish a baseline level of protection. The authors conclude that the FTC should police the term "privacy policy" to provide a more uniform understanding of the term (Turow, 2006).

A third evaluation of current FTC policy was conducted by the Electronic Privacy Information Center (EPIC), a Washington DC based public interest center devoted to civil liberties and privacy protection. EPIC published a report in 2005 titled "Privacy Self-Regulation: A Decade of Disappointment." The report focused on the self-regulation initiative outlined in the 1996 FTC report. EPIC concludes that much like the self-regulation of telemarketing that occurred prior to the establishment of the national Do-Not-Call registry, industry self-regulation of privacy is failing. EPIC contends that spy-ware has become more prevalent under the self-regulation initiative. Spy-ware is software installed on a consumer's computer, often without their knowledge, that is intended to collect personal information and report it back to a particular company. "Decade of Disappointment" calls on the FTC to regulate online privacy much the same way the UPenn report recommends, by establishing a baseline of protection that consumers can expect and trust. EPIC also cites the Fair Information Practices as an example of such a baseline.

The EPIC report concludes that the insufficient privacy practices occurring online and in electronic form are also finding their way into the offline world as well. The report points to cashiers asking for a customer's phone number. Stores that collect phone numbers are then able to tie purchasing habits to the customer's phone number and use that information for telemarketing, direct mailing, or even for sale to other companies. Another example provided was the use of loyalty cards or shopper's club cards that track consumer buying habits. The cards are often touted as providing discounts, when in fact; the EPIC report demonstrates that prices often remain comparable to other stores, but the collecting store gains valuable information about their patrons. The most unsettling of

these trends according to EPIC is the impression that handing over this personal information is a pre-condition for sale. In other words, customers feel obligated to provide their personal information in order to be able to purchase goods or services (EPIC, 2005).

Proposed U.S. Laws

The proposed laws covered in this section are not meant to be an all-encompassing list, but a representation of the types of laws being proposed to deal with consumer privacy concerns. Four proposed laws were selected for review in this chapter. Before making a recommendation regarding how the U.S. might move forward with privacy legislation, it is important to look at the solutions that have already been considered. The selection was made by searching proposed laws available on Thomas.gov, the Library of Congress site that provides a searchable database of proposed laws that are currently under review by Congress.

A search of Thomas.gov provided several proposed laws dealing with privacy concerns. Only a small number contained the type of wide-ranging solution discussed in this research. The following proposed federal laws, listing in Figure 2C, will be examined and analyzed for their ability to fulfill the Fair Information Principles.

Figure 2C: Examples of Proposed U.S. Privacy Legislation

- Consumer Privacy Protection Act of 2005
- Personal Data Privacy and Security Act of 2007
- Privacy Act of 2005
- Privacy Rights and Oversight for Electronic and Commercial Transactions Act of 2006 (PROTECT Act)

Each of these proposed laws deals directly with commercial businesses and their interactions with consumer personal information. Each one will be summarized and examined for its ability to implement the Fair Information Practices already followed by federal government agencies.

Consumer Privacy Protection Act of 2005

Proposed by representative Clifford Stearns (R-FL), the Consumer Privacy Protection Act of 2005 requires companies to produce and make available a notice to consumers that the company may use their collected information for purposes different than what was originally intended, if applicable. The mandatory privacy statement must also be clear, concise, and in "plain language." The statement must be available to all customers at no charge and must provide the following (see Figure 2D). Finally, the proposed law requires that companies have a security plan to maintain appropriate levels of protection for consumer personal information.

Figure 2D: Consumer Privacy Protection Act Statement Requirements

- The types of information that may be collected
- How the information may be used
- Whether or not the consumer is required to provide information in order to do business with the company
- The extent to which the information is for sale or may be shared
- Opportunity to limit use to that which is required to complete the transaction
- Ability to limit sale of the information to a 3rd party for 5 years

The Consumer Privacy Protection Act of 2005 puts into law the de facto state of the industry which has already been shown to be unacceptable. The proposed legislation would make it mandatory to provide the same privacy policies that the majority of

companies already make available through their websites. The only significant improvement would be the mandatory notice from companies to consumers that the company is changing what they will use the information for, although the ability to "opt-out" of certain uses would be statutorily limited to 5 years. After which, the consumer would have to re-affirm that they did not want the company to use the information for purposes different than those originally intended (Consumer Privacy Protection Act of 2005).

Personal Data Privacy and Security Act of 2007

Proposed by Senators Leahy, Specter, Feingold, Schumer, and Sanders, the Personal Data Privacy and Security Act of 2007 provides for possible fines and incarceration for organizations found guilty of concealing a breach of personal information security that resulted in the possible exposure of personal information to unauthorized persons. With a maximum sentence of 5 years, the law does provide a significant incentive to notify the public of breaches. The proposed law also places specific requirements on data-brokers, or companies that trade in personal information. Under the proposed law, data-brokers must provide individuals access to their file for a reasonable fee, as well as instruction of how to obtain access to their files and a way to make corrections. The proposed law also requires heads of government agencies to conduct a Privacy Impact Study prior to purchasing information from or engaging in a contract with a company considered to be a data broker. Government agencies would also be required to designate a full-time privacy officer, charged with maintaining the

agencies' adherence to federal privacy policy that would report to the deputy attorney general.

The Personal Data Privacy and Security Act do have wide-ranging impact. Not only does it mandate privacy policies that specifically address privacy concerns, but it requires that notification be provided to consumers when there is a breach and makes failure to do so a punishable crime. The creation of privacy officers within each federal agency and the requirement to conduct privacy studies is possibly progressive, but the results of those actions are uncertain and beyond the scope of this research.

Unfortunately, the remainder of the law is specifically targeted at data-brokers and provides them with several exemptions. The proposed law exempts certain important information from being considered under the restrictions. A consumer's purchasing history, which is considered very private, is exempt from the restrictions as well as any aggregate or proprietary data developed from analyzing the personal information. This exemption leaves major holes in the protection offered.

The Personal Data Privacy and Security Act of 2007 continues the trend of tailoring privacy legislation to a specific industry instead of applying a uniform standard across all industries, which would be beneficial for consumers. The protections offered by this proposed legislation are severely limited by exemptions and exceptions provided to data-brokers.

Privacy Act of 2005

Proposed by Senator Feinstein (D-CA) the Privacy Act of 2005 requires the consent of an individual prior to the sale of their data, or before data is provided to a third

party for marketing purposes. The law does not; however, prevent a company from collecting personal information without consent for its own marketing purposes.

Notice must be given prior to the sale or use of the personal information and with a reasonable period of time for the consumer to consider the notice and limit such sale or use. The proposed law would also mandate the notice provided to the consumer contain several components (Figure 2F).

Figure 2E: Requirements for Privacy Act 2005 Notice

- The identity of the collecting entity
- Types of information being collected
- How the entity may use that information
- A description of possible third parties that may receive that information
- Whether the information collected is necessary to do business with the entity
- How the consumer may go about declining to have their information sold to or used by a third party

This proposed legislation by Senator Feinstein contains language similar to the Consumer Privacy Protection Act proposed the same year. This proposed law addresses only the Notice and Choice principles of the Fair Information Principles; which does not meet the desired results outlined by the FTC or those desired by consumers.

Senator Feinstein continues to work toward greater protection for consumers against identity theft and fraud. Her website discusses additional proposed legislation that would require notice from both federal agencies, as well as companies when breaches in their security have occurred, which may put at risk the personal information of consumers. While well-intentioned, these new proposals continue the piece-meal approach that has been shown by the FTC's own reports and the Annenberg Report to be confusing to consumers.

PROTECT Act of 2006

The Privacy Rights and Oversight Electronic and Commercial Transactions Act of 2006 (PROTECT Act) was proposed by Senator Hillary Clinton (D-NY). On her website, Senator Clinton describes the need for such legislation:

> At all levels, the privacy protections for ordinary Americans are broken, inadequate and out of date. It's time for a new comprehensive look at privacy. We need consumer protections that are up to date with the technological and national security needs of our time, for a world in which we can be confident that our security and our privacy are both protected," said Senator Clinton. "We can protect our privacy in a more data driven and dangerous world. This issue is too important to be dealt with haphazardly or not at all. We need to stand by our cherished American ideals and think intelligently about how they apply in this new century. (www.senate.gov, 2007)

Senator Clinton's proposed legislation would make it illegal for companies to allow personal data in their possession to be compromised through theft, loss, or data breach. The proposed law would levy penalties as high as $1,000 per individual affected or up to one percent (1%) of the company's overall annual revenue. In addition, providing credit information to an unauthorized individual could result in penalties of $5,000 to the injured individual or up to five percent (5%) of the company's annual revenue. Small businesses would be exempt from these rules and not expected to pay these kinds of fines. Senator Clinton's proposal would also establish a series of protections aimed at

notifying consumers of breaches that may affect their personal information and provide them with tools to combat identity theft after breaches occur (PROTECT Act).

The proposed PROTECT Act would also establish a Chief Privacy Officer or Clinton described "Privacy Czar" (Kornblut 2006) in the Office of Management and Budget (OMB). The so-called privacy czar would only have jurisdiction over federal agencies and be charged with ensuring compliance with the Privacy Act of 1974. The privacy czar would have no control or authority over companies.

The PROTECT Act does offer some recourse to those individuals who fall victim to identity theft due to company negligence. However, beyond that protection, the proposed legislation would offer little beyond restating the Fair Information Principles, already well established, without providing real enforcement of those principles.

Chapter Summary

Research conducted by EPIC, the University of Pennsylvania, and the Federal Trade Commission itself conclude current U.S. policy is not effective at protecting personal information. All three also conclude the best method of dealing with the current deficiencies in consumer privacy protection is to pass legislation or enforce mandatory regulations in order to establish a baseline of consumer protection based on the Fair Information Practices, which were originally recognized by the Secretary's Advisory Committee on Automated Personal Data Systems in their report to the Secretary of Health Education and Welfare (HEW) in 1973.

This chapter also outlined four proposals that have been presented to Congress in the last several years. None of the proposals examined are sufficient to address the

public's concerns or to enforce the Fair Information Principles established in the 1974 HEW report. To date, none of the examined proposals has been made into law.

In 2000 the Canadian Parliament passed the Personal Information Protection and Electronic Documents Act (PIPEDA), which is designed around the Fair Information Principles and has achieved significant success. The next chapter will examine PIPEDA and the current state of privacy policy in Canada with the intent of analyzing PIPEDA's ability to provide a template for successful privacy policy to be used in the U.S.

Chapter 3: Canada as a Comparison

A 2006 survey of Canadians conducted by the Ponemon Institute indicated eighty percent (80%) of Canadian citizens believe privacy to be important or very important. Among their primary privacy concerns were identity theft and contact from unwanted telemarketers (Ponemon, 2006). Canada is the United States' primary trading partner, with over $500 billion in trade each year, and personal information about citizens of both countries crosses the border each day (census.gov, 2008). The previous chapter discussed the U.S. approach to privacy and changes proposed by U.S. lawmakers. This chapter will examine the Canadian approach to privacy policy and its results.

Canada's Approach to Privacy Policy

On April 13, 2000, Canada's parliament passed into law the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA was created to address consumer concerns about their personal information collected and used by private organizations. These concerns are very similar to those expressed by U.S. consumers. The Canadian Privacy Commissioner states "The Act [PIPEDA] establishes rules for the management of personal information by organizations involved in commercial activities." While the Canadian Parliament had already addressed the issue of personal information held by the federal government with the Privacy Act of 1983, they took it one step further by applying similar rules to the corporate world. According to the Privacy Commissioner's website, "The Act [PIPEDA] strikes a balance between an individual's right to the protection of personal information and the need of organizations to obtain and

handle such information for legitimate business purposes." The Commissioner goes on to state the Act [PIPEDA] creates rules for the management of personal information (privcom.gc.ca, 2008).

These statements are important because they carry the underlying assumption that businesses should only collect information when it has an immediate business purpose and that information needs to be managed in an appropriate fashion. This may seem obvious, but in many cases companies store personal information on the chance that it may someday become useful. Companies have also been found to use personal information in an insecure fashion that leaves it vulnerable to abuse. One such case involved the Canadian Imperial Bank of Commerce (CIBC) faxing personal information to incorrect numbers for three years before catching the error (Pitts, 2005).

PIPEDA rules that "an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." In other words, PIPEDA mandates that organizations (e.g. companies, non-profits, and non-governmental organizations) only collect personal information about an individual when it is necessary for that organization to do so for the successful operation of its business.

PIPEDA expects organizations to abide by a set of principals developed under the Canadian Standards Association's *Model Code for the Protection of Personal Information*, recognized as a Canadian national standard in 1996. The code describes ten standards which are outlined in Figure 3A.

Figure 3A: Summary of Model Code for the Protection of Personal Information

- **Accountability:** Organizations have to designate a privacy officer and take responsibility for the personal information they maintain.
- **Identifying Purposes:** Organizations have to decide what information they maintain and why it is appropriate.
- **Consent:** Organizations must have the consent of individuals before they can collect, use or distribute their personal information.
- **Limiting Collection:** Only collect the information identified as necessary for business.
- **Limiting Use, Disclosure, and Retention:** Restrict the collection, use and distribution of personal information to the minimum extent feasible.
- **Accuracy:** Personal information must be accurate, complete, and up-to-date.
- **Safeguards:** Personal information must be protected by security safeguards appropriate to the sensitivity of the information.
- **Openness:** Organizations inform individuals of their policies and practices relating to the management of personal information.
- **Individual Access:** Upon request, an individual must be made aware that information has been collected and be provided access to that information. Individuals are able to challenge the accuracy and completeness of the information and have it amended as appropriate.
- **Challenging Compliance:** An individual must be able to challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

(http://www.csa.ca/standards/privacy/code/Default.asp?language=english , 2008)

The above standard is designed to maximize transparency and allow individuals to be aware of who is collecting their personal information, for what reason, and what is being done with that information. The standard also makes it clear that personal information should be regarded as something that requires protection and should receive careful stewardship. The *Model Code for the Protection of Personal Information* is very similar to the Fair Information Principles developed under the U.S. HEW report of 1973, which is because the HEW report served as a model for those at the Canadian Standards Association when the *Model Code for the Protection of Personal Information* was developed (privacyrights.org, 2007).

The Privacy Commissioner of Canada

The *Model Code for the Protection of Personal Information* defines a procedure for how personal data should be collected, stored and distributed. When that procedure and associated legislation are not followed, PIPEDA also has its own executive agency to pursue cases or abuse. The Canadian Privacy Commissioner reports directly to Parliament and is the highest level privacy officer in Canada. The Privacy Act and PIPEDA installed the Privacy Commissioner as the primary defender of Canadian's privacy rights. Canadian privacy laws (Privacy Act and PIPEDA) provide the commissioner with several rights and powers (Figure 3B).

Figure 3B: Rights/Powers of the Canadian Privacy Commissioner

- Investigating complaints and conducting audits;
- Publishing information about how personal information is handled in the public and private sectors;
- Conducting research into privacy issues; and
- Promoting awareness and understanding of privacy issues by the Canadian public.

The Commissioner works independent of other government agencies to investigate privacy complaints from individuals about either the public or private sector. The Commissioner states:

> As an ombudsman, the Commissioner prefers to resolve complaints through negotiation and persuasion, using mediation and conciliation if appropriate. The Commissioner has the power to summon witnesses, administer oaths and compel the production of evidence if voluntary co-operation is not forthcoming (tbs-sct.gc.ca, 2003).

The Commissioner may have the right of subpoena and a respectable amount of persuasion power, but the office does not have the power to enforce privacy laws. If an organization refuses to follow the recommendations of the privacy commissioner, the matter can be referred to the federal court system, which can review the case and enforce the law accordingly. Any evidence collected by the privacy commissioner can be admitted to federal court cases.

The Commissioner's report outlines improvements to industries such as banking, telecommunications, and insurance that have been under PIPEDA's authority since 2001. Other industries such as law firms and the retail sector have a weaker record on PIPEDA compliance but PIPEDA has only applied to these industries since 2004. The Office of the Privacy Commissioner uses the difference to demonstrate the success over time of PIPEDA. The longer an industry must comply with PIPEDA, the higher the success rate. At the same time, the report authors implore industry to take greater steps toward compliance with all parts of PIPEDA, including the issues of notice and consent which are harder to address (OPC, 2007).

In describing its other efforts, the Privacy Commissioner's report also states over $900,000 in research funds has been awarded by the Commissioner to various university and non-profit researchers to work on privacy topics of concern. The Privacy Commissioner reports positive research results and intends to fund additional proposals in 2007 and 2008, specifically in the areas of personal information on the internet; secure identification and authentication, and the intersection of public and private sector concerns (OPC, 2007).

The Commissioner's report discusses the current weaknesses of PIPEDA and areas for improvement. Along with cross-border transfers, the Commissioner would like to see increased Parliamentary involvement regarding intrusive technologies, the extensive information gathering conducted by the private sector, breach notification and the government's access to the information collected by private sector organizations. The Commissioner believes these areas of policy need the most attention and enhancement. The Commissioner also believes that Parliament should repeal the 2002 Public Safety Act that provided greater access to information and more numerous policy loopholes for law enforcement. It is the position of the commissioner that there are already sufficient considerations for law enforcement and the Public Safety Act unnecessarily extends allowances for law enforcement (OPC, 2007).

The 2006 Annual Report from the Office of the Privacy Commissioner also offers room for improvement, and states that PIPEDA is a necessary and successful piece of legislation that is making great strides toward providing the level of privacy protection being demanded by the Canadian population. Several third party organizations have also conducted their own reviews of PIPEDA in various forms. The next section will explore these other reports and compare their conclusions to those of the Privacy Commissioner.

Privacy Cases

In 2003, Jennifer Stoddart became the second Privacy Commissioner of Canada. Commissioner Stoddart's seven year term charges her with being an ombudsman responsible with investigating complaints, making findings and issuing non-binding recommendations concerning privacy issues. The majority of complaints brought before

the Commissioner are resolved by the litigants on their own, or through recommendations from the Commissioner's office. According to the 2005 Annual Report, the Commissioner's Office closed over 400 complaints filed under PIPEDA, or on average it takes the Commissioner's Office 11 months to close a case. Of those cases, one-fifth were decided to be not founded. This does not mean the remaining four-fifths were well-founded. Some cases, approximately 4 percent, were resolved through early resolution. In these cases, the company independently satisfied the complainant in some fashion. In over half the cases, the complaint was either "Resolved" or "Settled" between the company and the complainant, which indicates strong, positive results.

The statistics provided in the Privacy Commissioner's annual report offer information about the success of the Privacy Commissioner's Office; but examining individual cases can provide context. The Commissioner's office classifies cases by the type of complaint. Some cases are categorized as collection issues. In such cases, the complainant charges that an individual or organization is improperly or unnecessarily collecting personal information. One such case involved a student that complained he had to provide his SIN (Social Insurance Number, equivalent to U.S. SSN) in order to rent an apartment. The apartment owner required renters to provide their SIN for identification purposes as well as for use in credit checks and collections. In this case PIPEDA allows for the collection of SINs with the permission of the providing individual. The SIN cannot, however, be a condition for service. The apartment owner is not allowed by law to refuse to rent based on whether or not a renter provides his/her SIN number. The apartment owner agreed to change his policy and now only requires a driver's license as identification.

Other cases reviewed by the Privacy Commissioners office are considered access problems. In these cases the complainant has requested access to their information kept by an organization and been refused. In one such case, an individual provided a business with a written request to access the information the organization maintained about the individual. The complainant was provided with some of the information but denied access to information that was collected prior to January 1, 2004. The organization's reasoning was that this information pre-dated PIPEDA and was not subject to the law. The individual had also requested access to a copy of the company's privacy policy, which was also denied. Once the Privacy Commissioner's office became involved, the remainder of the individual's information was provided and it was learned that the organization did not have a privacy policy. Upon request from the Commissioner's Office, the organization created a privacy policy and presented it to the complainant.

Some cases are resolved over the course of the investigation and the gathering of case facts. One such case involved an organization's policy of requesting one additional form of identification, beyond the membership ID, for access to member discounts. This policy was created to ensure members were not letting friends or relatives borrow their membership IDs in order to obtain the benefits without being a member. The Commissioner's Office found that no one particular form of supplemental ID was being required; it was up to the individual member to prove who they were. The supplemental information was also not being stored in any way. The Commissioner's Office explained that the organization was not in violation of PIPEDA and the complainant was satisfied with the result.

The three cases outlined above, along with the statistics provided in the Commissioner's annual report indicate a positive track record for PIPEDA. While not every organization that falls under PIPEDA has fully complied with the law, they generally appear eager to correct problems that are identified. Conversely, according to a report issued in 2006 by Ryerson University in Ontario, privacy issues just are not on the radar for most organizations. While there was significant concern that PIPEDA would create a storm of information requests and complaints, that storm has failed to materialize after two years. The benefits of PIPEDA appear to be significant.

Privacy International 2006 Study

The Canadian Privacy Commissioner's Annual Report warned of the continuing threat of cross border transfers that often puts Canadians' personal information at risk for collection and use by companies and governments that are not obligated to adhere to PIPEDA. While Canada's PIPEDA provides significant protection to Canadian consumers, several of its trade partners, including the United States are not as well-respected internationally for their protections.

Canada was among Privacy International's two highest ranked countries in terms of privacy protection world-wide in 2006. The United States, however, did not receive such high marks and was rated among the worst privacy offenders. The Privacy International Report looks at several key indicators for privacy protection (Figure 3C).

Figure 3C: Criteria for Privacy International Rankings Report 2006

- Constitutional protections
- Statutory protection
- Privacy enforcement
- Identity cards & biometrics
- Data sharing provisions
- Visual surveillance
- Communications interception
- Workplace monitoring
- Law enforcement access
- Data retention practices
- Travel & finance surveillance (including trans-border data sharing)
- Global leadership
- Democratic safeguards

After examining a group of 37 countries that included most of Europe, North America, and the major countries of Asia, Privacy International provided some significant findings (Figure 3D).

Figure 3D: Privacy International 2006 Summary of Key Findings

(Please note that "worst ranking" and "lowest ranking" denotes countries that exhibit poor privacy performance and high levels of surveillance.)

- The two worst ranking countries in the survey are Malaysia and China. The highest-ranking countries are Germany and Canada.
- In terms of statutory protections and privacy enforcements, the U.S. is the worst ranking country in the democratic world. In terms of the health of national privacy protection, the U.S. has been ranked between Thailand and Israel.
- The worst ranking EU country is the United Kingdom, which fell into the "black" category along with Russia and Singapore. The black category defines countries demonstrating "endemic surveillance."
- Despite having no comprehensive national privacy law, the United States scored higher than the UK. Thailand and the Philippines also scored higher than the UK.
- Argentina scored higher than 20 of the 25 EU countries.
- Australia ranks higher than Slovenia but lower than Lithuania and Argentina. New Zealand ranks higher than Australia and has an equivalent ranking to the Czech Republic.

The Privacy International results present a stark contrast between the United States and Canada in terms of privacy protections. Canada was ranked as one of the two best countries in terms of privacy protection, while the U.S. was considered the "worst ranking country in the democratic world (Privacy International, 2006)." The Privacy International findings seem to substantiate the concern of the Canadian Privacy Commissioner. The transfer of Canadian consumers' information across borders to other countries, especially the U.S., will almost certainly risk weaker protections for that information.

Additional Reviews of PIPEDA

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) is located at the University of Ottawa. The Clinic seeks to ensure balance in policy and the law-making processes on issues that arise as a result of the development of new technologies (cippic.org, 2007). In 2006, CIPPIC released a report, titled "Compliance with Canadian Data Protection Laws: Are retailers measuring up?" examined the Canadian online retail industry for compliance with the rules of PIPEDA. The retail industry has been obligated to follow PIPEDA's rules since 2004 and was cited by the Privacy Commissioners Annual Report as deficient. CIPPIC research discovered widespread non-compliance among the over 70 online retailers they reviewed; several failed to fulfill even basic statutory requirements, such as posting the name and contact information of the individual in charge of privacy at the company (CIPPIC, 2006).

In addition, the report on the retail sector found that between one-half and two-thirds of the retailers they reviewed share customer information with third parties even

when that sharing is not required to complete the transaction. Researchers found customer service representatives to be very poorly educated regarding their company's privacy policies and procedures. Researchers experienced long delays or no responses to inquiries for privacy information; as many as one-third of requests for information from retailers went unanswered. Finally, the report concluded that when it came to obtaining customer consent, retailers' methods failed to meet the minimum requirements defined by PIPEDA (CIPPIC, 2006). The report verifies that industries such as online retail, that have only been required to comply with PIPEDA for less than two years are not fulfilling their obligations to Canada's consumers.

While the CIPPIC report details limited success achieved by PIPEDA among industries with less than two years of required compliance with the law, a report conducted by the Canadian trade organization, NYMITY offers another perspective. NYMITY Inc. provides privacy consulting and services to organizations desiring to increase their compliance with Canadian privacy laws. In 2006 NYMITY released their annual report in conjunction with the Canadian Marketing Association (CMA) titled, "Trends in Transparency." By examining the top 20 to 30 companies in each of the selected industries NYMITY was able to identify a variety of trends (NYMITY, 2006).

NYMITY's report indicates an apparent difference between those industries that have been governed by PIPEDA since 2000 and those that have only recently had to comply (since 2004). Privacy policies of companies in banking and telecommunications had extensive privacy policies, which were on average 10 to 14 pages in length, conversely companies in the retail sector averaged a brief 4 pages. Twenty one percent (21%) of customer services companies surveyed utilized privacy seals and eighty seven

percent (87%) of the banking sector provided toll-free numbers for customers to opt out of sharing policies. One statistic of particular note is that eighty two percent (82%) of all the companies NYMITY surveyed in 2006 had privacy policies that applied to all company business instead of being limited to online transactions (NYMITY, 2006). The significance of the eighty two percent (82%) becomes apparent when it is compared to U.S. companies in the privacy policy analysis section of this thesis.

Chapter Summary

While the CIPPIC reports demonstrate that further progress must be made with privacy in Canada, the Privacy Commissioner's annual report and the findings by NYMITY show that significant progress is being made within industries that have only been subject to PIPEDA for fewer than 5 years. While the FTC is reporting failure after over a decade of current policy efforts, PIPEDA is experiencing success after less than half that time.

In the United States the Federal Trade Commission (FTC) chose to pursue three initiatives; enforcement of existing laws, industry self-regulation, and consumer and business education. After more than a decade this system has failed to achieve the desired results. Canada chose a different route and pursued legislation aimed at establishing a baseline standard for privacy protection implemented at the federal level and under the leadership of a national Privacy Commissioner. Unlike the American initiative, the Canadian law (PIPEDA) seems to be succeeding after only a few years.

Chapter 4: Research Questions

The previous chapters explored the current privacy situation in both the United States and Canada. The reports issued by the FTC, Annenberg School for Communication, and the Electronic Privacy and Information Center (EPIC) all demonstrate a clear failure of U.S. privacy policy to fulfill the goals outlined by the U.S federal government for consumer privacy protection called the Fair Information Principles. Legislative proposals for change also do not seem to address the problems with the current policy. The review of pending legislation showed a lack of ideas for addressing the Fair Information Principles. Proposed legislation continues the piece-meal approach to privacy legislation that has been criticized in the literature, and fails to mandate adherence to the Fair Information Principles.

At the same time, Canada's federal law, PIPEDA, is experiencing some success. Based on the Fair Information Principles, PIPEDA was designed to provide the level of protection desired by both U.S. and Canadian consumers. However, in order to determine if legislation similar to PIPEDA would be beneficial in the United States, the following questions must be answered.

Question 1 - Is Canada's Privacy Policy (PIPEDA) more effective than U.S. policy of industry self-regulation at achieving the Fair Information Principles in company privacy policies?

Before adopting privacy policy similar to PIPEDA, one must understand PIPEDA's impact on industry privacy policies as they apply to all of the Fair Information

Principles. If the stated goal is to create policy that will fulfill the FTC's goal of providing consumers with the level of protection described in the Fair Information Principles, then it is important to understand how PIPEDA makes industry privacy policies in Canada different from those in the United States. Does PIPEDA change the balance between individual rights and marketplace forces?

Question 2 - Should PIPEDA be used as a model for future U.S. privacy policy, and if so what lessons can be learned from its nearly seven year history?

If it is found that PIPEDA is achieving the desired results and is worthy of consideration when implementing future U.S. privacy policy, it would be a mistake to simply copy PIPEDA in its entirety. Through this research, lessons will be learned regarding PIPEDA's strengths and its weaknesses. The privacy policy analysis and stakeholder analysis will provide insight that should be strongly considered when creating privacy policy to address the needs of the United States. Since PIPEDA focuses on the rights of the individual, consideration must also be given to the other driving forces, of the marketplace and security in any recommendations.

Question 3 - Who are the critical stakeholders concerned with U.S. privacy policy and how do their positions impact future policy changes?

U.S. stakeholders must be considered in the development of any new privacy policy. Effective privacy policy must accommodate the needs of more than one party in

order to provide an overall benefit to the country. It is unrealistic to believe privacy policy can be built around only U.S. consumers without considering the impact it will have on both government and industry. It is worth examining the corresponding stakeholders in Canada to see how changes to Canada's privacy policy have impacted them.

Question 4 - Would a change in policy similar to PIPEDA impact various U.S. industries in different ways and if so are those impacts significant enough to be considered when adopting future privacy policy?

It is essential to consider the impacts of PIPEDA on a variety of industries and whether or not PIPEDA may produce undesired effects on essential industries. Historically U.S. privacy policy has been tailored to individual industries or circumstances. It is important to understand how more broad based policies will impact industries differently. For example, under Canada's system the banks and telecommunications industries have faced special focus because their businesses routinely transfer data across the border to the U.S. Canadian companies in the banking and telecommunications industries are under additional pressure to protect the information of Canadians.

Chapter Summary

This chapter lays out four research questions. The answers to those questions may provide critical information for U.S. policymakers looking to create new privacy policies

or modify the existing policy. Chapter 5 will outline the methodology that will be used to answer the four research questions as well as some explanation as to the choice of research methodology.

Chapter 5: Methodology

The literature review conducted for this thesis outlined the current state of federal privacy policy as it applies to companies in the United States and Canada. The purpose of the literature review was to demonstrate the significant problems with the current U.S. privacy policy and the apparent success achieved by Canadian privacy policy. The literature review also examined some of the proposals for change being considered by the U.S. Congress. The proposals that were reviewed appear to be both inadequate to address the goals of the FTC and unlikely to be passed into law.

In order to answer the research questions detailed in Chapter 4, two different methodologies will be employed. A content analysis will answer the primary research questions as to which country has company privacy policies which are more closely aligned with the Fair Information Principles and is PIPEDA a good model for change in the United States. Individual company policies will be compared to the Fair Information Principles and to the privacy policies of other companies.

The second evaluation method of *stakeholder analysis* will answer the third and fourth research questions, regarding how changes in privacy policy may affect stakeholders differently and how stakeholders' positions may impact privacy policy. Some stakeholders may benefit from a change in privacy policy while others may find the current policies more beneficial. As part of the analysis, several specific case studies will be reviewed to provide a complete picture of how the different countries' privacy policies are implemented and the effects those implementations have on the stakeholders involved.

The Importance of Privacy Policies

Consumer education about privacy is a primary goal of current U.S. privacy policy. The primary method to educate people is through online privacy statements posted by organizations on their websites. Consumers are able to visit the company's website and view their privacy policy. The privacy policy link is usually found in the header or footer of the website and is available on every webpage on the company's site. Website privacy policies are easily obtained in a short period of time with an internet connection.

The Annenberg report published in November 2006 stated that, "Large majorities of consumers believe that the term 'privacy policy' [on an organization's website] conveys a baseline level of information practices that protect their privacy" (Turow, 2006). Consumer assumptions are incorrect, as demonstrated in the Literature Review.

Privacy Policy Content Analysis

The responsibility for implementing privacy policy changes lies with companies. Individual company privacy policies reflect the implementation of each country's privacy legislation. A privacy policy content analysis will be conducted to evaluate companies that conduct business in both the United States and Canada in order to contrast their privacy policies in both countries. The content analysis technique involves comparing the statements made in a company's privacy policy with the goals outlined in the Fair Information Principles. The goal of the content analysis will be to answer the first research question: Is Canada's Privacy Policy (PIPEDA) more effective than U.S. policy of industry self-regulation at achieving the Fair Information Principles? The content

analysis will also provide insight that will help answer question 2: Should PIPEDA be used as a model for future U.S. privacy policy, and if so what lessons can be learned from its nearly seven year history?

In order to make this comparison, privacy policies have been collected from a sample of companies that do business in both the United States and Canada, as well as some companies that only have privacy policies applicable to U.S. consumers. Companies were selected based on three criteria; first, companies were chosen from the Fortune 500 listing of biggest companies. Second, a smaller list of companies was selected from the Fortune 500 list based on their industry's high level of customer interaction. Industries with high levels of customer interaction are those that need to collect individual customer information to conduct their business or those that are regularly exposed to individual customer information. These selections were based on the researcher's best judgment. Third, some companies were included from outside of the Fortune 500 list because of their presence in the media as they related to privacy issues. During the literature review, companies such as LexisNexis and ChoicePoint continued to reappear in the news following privacy concerns. These companies were selected for consideration based on their high profile in the privacy debate.

Figure 5A: Company Selection Criteria

- Fortune 500 (Fortune Magazine)
- Level of consumer interaction
- Media presence (controversies, criminal cases, etc.)

The Fortune 500 listing is a ranking of the top 500 American public corporations (by revenue), published by *Fortune* magazine on an annual basis. The Fortune 500

companies represent the biggest publicly owned companies in their respective industries. These companies are the trend-setters and are used for the purpose of this thesis because they represent the status-quo of their industries. The Fortune 500 listing includes companies in industries such as defense and energy, which have little interaction with consumers on a regular basis. Those types of companies were not included in this analysis, unless they met the last criteria.

Other companies were included that may not be large enough to make the Fortune 500 listing, but are nevertheless important to this analysis because of their media coverage as it relates to privacy issues. Companies, such as ChoicePoint and LexisNexis have made headlines over concerns regarding their handling of consumer data. It is essential to examine these companies for situations occurring under American law that may be avoided under Canadian law. The table below (Figure 5B) lists the industries from which company selections were made for inclusion in this content analysis.

Figure 5B: Industries selected for analysis

- Banking
- Data Brokering
- Financial Services
- Insurance
- Internet Retail
- Advertising
- Online Services
- Restaurants
- Shipping
- Telecommunications

Many of the companies in the selection conduct business in both the United States and Canada. A company conducting business in both countries may choose to meet the requirements of the different countries in a single policy, or in separate policies which is

more common among those selected analysis. These companies may choose to have a separate website for the Canadian operations with a .ca extension instead of the typical .com extension. For example, American customers are accustomed to accessing www.amazon.com, but Amazon also has a Canadian version at www.amazon.ca. Among websites such as Amazon, it is also common to have differing privacy policies. Canada's PIPEDA has certain requirements that must be met by companies conducting business in Canada, while U.S. privacy policy focuses on a system of industry self-regulation.

Criteria for Analysis – Privacy Policy Rating System (PPRS)

To analyze the selected privacy policies, they were first divided between those that apply to U.S. customers and those that apply to Canadian customers. In some cases the same policy applied to both countries, in which case the same privacy policy was considered as both an American privacy policy and a Canadian privacy policy. Each set of privacy policies was then compared against a set of principles developed for this study, which are based on the 1973 HEW report and more recent iterations (Figure 5C).

Figure 5C: Fair Information Principles developed for this analysis

Principle	Definition
Notice of Existence	The existence of recordkeeping systems and practices regarding collection of data should be publicly known.
Consent to Collection	Individuals should have control over collection of their personal information (except for purposes of law enforcement, etc.); and should consent to data being collected about them.
Limitation of Collection	No more personal information should be collected than is needed to complete a transaction.
Limitation of Use	Personal information should not be used for a purpose other than for which the purpose it was collected.
Retention of Data	Data should be retained no longer than necessary.
Access to Data	Individuals should have the right to access information about themselves. There should be a way for an individual to find out what information about him or her is contained in a record.
Accuracy of Data	Information that is kept needs to be accurate and complete. There should be a way for an individual to correct or amend a record of identifiable information about him or her.
Security of Data	There is a responsibility on the part of companies that maintain data to keep it secure. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of data.

Each privacy policy was compared against each principle and assessed a numerical value between 0 and 4 for each principle. The value indicates how well the privacy policy addressed the Fair Information Practice principle developed for this study. The values equate to the qualitative measurements defined by the researcher in Figure 5D.

Figure 5D: Definitions of Policy Ratings

Rating	Definition
0	Principle not addressed
1	Offers little protection and does not reflect the spirit of the principle
2	Offers some protection but does not reflect the spirit of the principle
3	Offers moderate Protection and reflects the spirit of the principle
4	Offers Good Protection and follows the spirit of the principle

Qualitative assessments are converted into quantitative ratings. The qualitative assessments were made by comparing the developed principles to the language used in the company's privacy policy. This method of "rating" the privacy policy was developed specifically for this analysis by the research and has been named the Privacy Policy Rating System (PPRS).

Figure 5E: Examples of Company Privacy Policy Ratings

0 = Principle Not Addressed
HSBC's privacy policy for U.S. customers does not address the principle, Retention of Data. "0" may be the easiest value to assess. If a principle is not addressed at all in the privacy policy, that policy receives a "0" value for that principle.

1 = Offers little protection and does not reflect the spirit of the principle
LexisNexis' U.S. privacy policy does address the principle of Limitation of Use; however the protection offered by the privacy policy is rather limited. LexisNexis' privacy policy for U.S. consumers offers little protection and does not meet the spirit of the Fair Information Practices, since it fails to prevent that information from being used for purposes other than the original intent. In this case the privacy policy received a value of "1" since it virtually did not address the spirit of the Fair Information Practice principle, Limitation of Use. LexisNexis may use gathered information for their own purposes, but they may also choose to share that information (without consent) with third parties who then in turn can combine that data with any other information they may have gathered. LexisNexis specifically mentions that they will share information with network advertising companies who are in turn permitted to do as they see fit with the data.

2 = Offers some protection but does not reflect the spirit of the principle
Wells Fargo's Canadian privacy policy does address the principle of Limitation of Collection; however the protection offered fails to reflect the spirit of the principle. The

privacy policy indicates that Wells Fargo will not necessarily limit the use of data which they collect to information pertinent to the transaction. They may also collect information that will be used for marketing by both Wells Fargo and also other service providers. Wells Fargo's privacy policy lists a limited number of reasons why they collect information, but it does not specifically limit what information is collected to provide the requested service to clients. In this case, the privacy policy received a value of "2" since it does provide some protection, but does not meet the spirit of the Fair Information Practice principle of Limitation of Collection.

3 = Offers moderate protection and reflects the spirit of the principle
Equifax's U.S privacy policy addresses the principle of Accuracy of Data and reflects the spirit of the principle. The privacy policy provides an email address for Equifax's customers to directly email their chief privacy officer with questions about their data. The privacy policy specifically mentions Fair Information Practices and the associated accountability. Equifax has provided customers with a method of inquiring about the data collected about them, but does not offer a specific option for altering that data. In this example the privacy policy received a rating of "3" since it reflects the spirit of the principle, and allows customers to verify their information even if it does not guarantee customers a way of easily changing their information.

4 = Offers good protection and follows the spirit of the principle
CitiFinancial's Canadian privacy policy addresses the principle of Consent to Collection and reflects the spirit of the principle. The privacy policy refers to CitiFinancial's practice of obtaining explicit customer consent prior to the collection or use of all personally identifiable information each time information is collected. In this case, the privacy policy receives a rating of "4" since not only does it reflect the spirit of the principle in its assurance of customer consent, but it provides good protection in that consent is obtained each time personally identifiable information is gathered.

The PPRS methodology will demonstrate which country's privacy policy is promoting company privacy policies more closely aligned with the Fair Information Principles. However, it is important to understand the effect that the different country's privacy policies have on the stakeholders involved. A stakeholder analysis will be conducted to provide additional context to the differences in national privacy policies.

Stakeholder Analysis

Question three of the research questions ask, "Who are the critical stakeholders concerned with U.S. privacy policy and how do their positions impact future policy changes?" The fourth question dovetails with that theme and asks, "Would a change in policy similar to PIPEDA impact various U.S. industries in different ways and if so are those impacts significant enough to be considered when adopting future privacy policy?"

Stakeholder analysis examines groups involved in the development and implementation of a policy in order to discover their motivations and influences they may exert to change the development of a policy or that policy's implementation (Brugha, 2000). For federal privacy policy in the United States and Canada, stakeholders can be broken down into government, industry and consumers (Figure 5F).

Figure 5E: Privacy Policy Stakeholders as Defined for Stakeholder Analysis

Stakeholder	Definition
Government	Any branch or service of a country's federal governing body, including legislators and executive agencies.
Industry	Any general business activity, commercial enterprise, or non-governmental organization.
Consumers	The general public that may or may not be customers of industry organizations, but are under the jurisdiction of government.

These three groups represent stakeholders that are directly impacted by privacy policy in the U.S. and Canada. These groups also play significant roles in the development and implementation of privacy policy. The government will create and enforce the policy while industry must implement the policies. It is the privacy of the consumers that is governed by the policy and it is up to the consumers to elect the government that creates the policy. This research will summarize some of the positions

held by representatives of these groups with interests in federal level privacy policy in order to determine key issues surrounding the topic.

Various opinions and perspectives exist within each of these stakeholder groups. The stakeholder analysis conducted will be accomplished at a summary level that will incorporate some of the topics of issue between the stakeholder groups. Within the government there are different agencies with numerous missions and positions towards personal privacy. Some examples of these differing missions and positions will be explored.

Within the industry group, the stakeholder analysis will highlight those company opinions that have been requested for congressional testimony as well as those positions that have been made public through statements published on company websites or through industry advocacy groups. The privacy policy analysis outlined earlier in this chapter will examine individual companies' published privacy policies in order to highlight any trends or patterns within industries or across all industries included.

Consumers also have varying opinions regarding how privacy should be treated by the government. The consumer section of the stakeholder analysis will examine the results of opinion polls and public opinion studies to obtain a general understanding of the position held by consumers. Groups of individual consumers also unite in the form of advocacy groups and watchdog organizations that advocate for consumers. Like industry advocate groups, consumer advocacy groups have also been asked to testify before Congress and their testimony will be examined to obtain a general understanding of how consumers are positioned in the privacy debate.

Criteria for Analysis - Uses

In addition to the scope of a policy and how it matched up to the baseline principles that is part of the content analysis, company privacy policies were also examined for the flexibility the individual policy provided the company. Although company privacy policies may be highly effective in protecting the privacy rights of consumers, such policies may severely restrict that company's ability to utilize information efficiently. The ability to gather, analyze, archive, and share information can be critical to the mission of a company and restrictive policies may not be desirable for the company stakeholder. This analysis examined the below uses companies may have for the information they collect and compared those uses to their privacy policies.

Figure 5F: Company Uses of Personal Information

Use	**Definition**
Gathering	Ability to gather information from the customer and from 3rd parties to produce a better product or better marketing/advertising
Analysis	Ability to manipulate the data in such a way as to extract the maximum amount of valuable information
Archiving	Ability to keep data as long as it will be useful
Sharing	Ability to share data with business partners or sell data for a profit

As part of the PPRS, each privacy policy was numerically rated (0-4) for each of the uses of information allowed by each company's privacy policy. The ratings are defined below (Figure 5G).

Figure 5G: Definitions of Information Use Ratings

Rating	Definition
0	Not addressed
1	Provides virtually no value to company
2	Extensive limitations that may impact mission/business operations
3	Some limitations imposed, but unlikely to impact mission/business operations
4	Company is permitted the maximum flexibility under the law

These quantitative measures were assessed by comparing the use defined in Figure 5F against the language of each company's privacy policy and assessing the policy a rating for each of the uses.

Figure 5H: Examples of Ratings

0 = Not Addressed

Firstdata's U.S. privacy policy does not address the principle of *Retention of Data.* This is the easiest value to assess. If the policy does not address the use at all in the privacy policy, that policy receives a "0" value for that category of use.

1 = Provides virtually no value to company
There were no "1" values assigned to any of the privacy policies for uses. A scenario in which a company would have personal information about a consumer and be so limited by their own privacy policy that the information provides the company with virtually no value does not seem likely.

2 = Extensive limitations that may impact mission
There were no "2" values assigned to any of the privacy policies for uses. Much like a "1" values, a company isn't likely to allow its own privacy policy to negatively impact its mission or business operations.

3 = Some limitations imposed, but unlikely to impact mission
Wal-mart's Canadian privacy policy received a "3" for *Sharing* of information. Wal-mart's privacy policy does not allow it to sell or rent personal information to third parties. While this may inhibit Wal-mart's business options, they are still able to use their customer information for their own benefit and for internal marketing of their products to customers. Therefore, Wal-mart's privacy policy imposes some limitations, but is unlikely to impact its overall mission.

4 = Maximum freedom within the law

LexisNexis' U.S. privacy policy received a "4" for *Gathering* of information. LexisNexis' business model involves the collection of personal information for the purpose of resale. Its business model requires it to collect as much information as legally possible in order to improve its product. Although LexisNexis has limited their posted privacy policy to their website, they include language that allows them to use cookies (an Internet tracking device) to gather information about visitors that can be used for future marketing purposes.

Case Studies

At the conclusion of the privacy policy analysis and the stakeholder analysis, the results will be discussed and several case studies will be examined closely. The case studies will include the results of the statistical analysis and the added context of the stakeholder analysis. Cases studies will include instances in which:

- A company's U.S. and Canadian privacy policies are identical
- A company's U.S. and Canadian privacy policies have significant differences
- The individual company privacy policy has caused specific problems for consumers

Chapter Summary

Multiple research methods will provide a better understanding of how U.S. and Canadian privacy policies differ in their implementation and their results. The privacy policy content analysis examines the actual results being achieved by the different countries' privacy policies. The stakeholder analysis reflects the key privacy policy stakeholders and how their influence affects privacy policy. Chapters 6 and 7 will reveal and examine the data collected by the privacy policy analysis and the stakeholder analysis respectively.

Chapter 6: Privacy Policy Analysis

The privacy statement on a company's website may only apply to that particular website and may not be indicative of all of the company's interactions with consumer personal information. Whether or not a company has chosen to post an all-inclusive privacy policy or a more limited policy is examined and incorporated into this analysis. This research will only examine those privacy policies available from the company's website since that is the policy most accessible to consumers and is the primary vehicle to inform consumers of a company's privacy policies. For each company, a copy of their privacy policy was downloaded from their American website and from their Canadian website, if one existed at the time of download. The content analysis examines company privacy policies to answer research question one and provide data that may help to answer research question four. By using the PPRS to compare the privacy policies of U.S. companies and their Canadian counterparts, the differences between the effects of the two country's laws will be highlighted. Should Canadian companies receive better PPRS scores, it can be inferred that Canadian law is doing a better job of achieving the Fair Information Principles. U.S. policymakers can then use this information to create more effective policy.

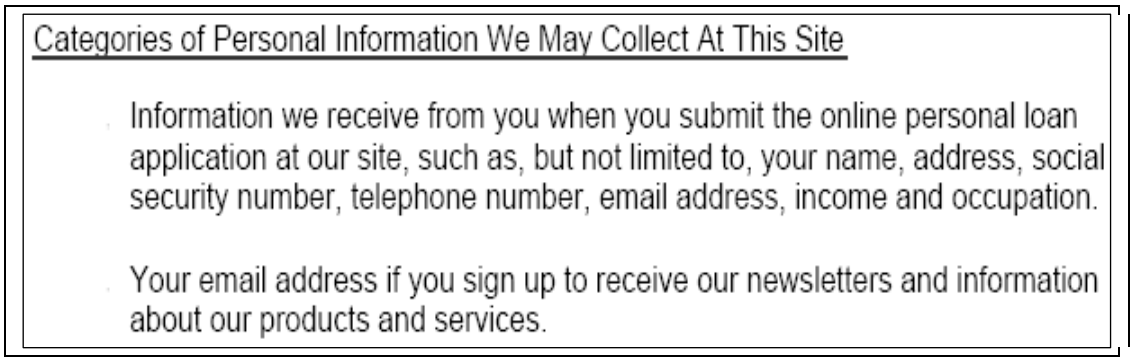
1. **Is Canada's Privacy Policy (PIPEDA) more effective than U.S. policy of industry self-regulation at achieving the Fair Information Principles?**

4. **Would a change [to in] policy similar to PIPEDA impact various U.S. industries differently and if so are those impacts significant enough to be considered when adopting future privacy policy?**

Forty two companies were selected for this content analysis. For each company, a copy of their privacy policy was downloaded from their American website, and if one exists from their Canadian website. In some cases one privacy policy is intended by the company to apply to consumers in both countries.

Context is important while reviewing the ratings given to each company's privacy policy. For example, the U.S. privacy policy for CitiFinancial received a "4" for the first principle of Notice of Existence. The privacy policy posted by CitiFinancial on their U.S. website only applies to transactions with the website and does not apply to other business interactions a consumer may have with CitiFinancial. While the rating of "4" is the best possible rating in this study, it does not automatically imply that that rating applies to all the business conducted by CitiFinancial. The rating only applies to the privacy policy posted on CitiFinancial's U.S. website and to the interactions between consumers and that website. The rating of "4" in this example was given since the privacy policy describes the existence of a collection of personal information and what that collection consists of (Figure 6A).

Figure 6A: CitiFinancial Notice of Existence



Categories of Personal Information We May Collect At This Site

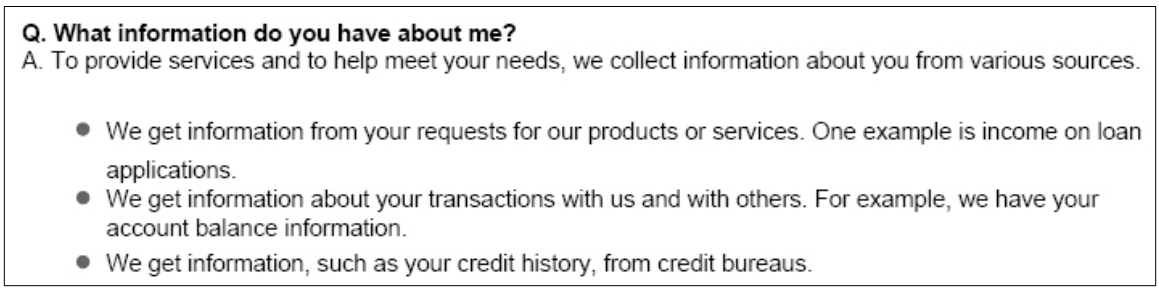
- Information we receive from you when you submit the online personal loan application at our site, such as, but not limited to, your name, address, social security number, telephone number, email address, income and occupation.
- Your email address if you sign up to receive our newsletters and information about our products and services.

(http://www.citifinancial.com/common/citigroup_privacy.php , 2007)

The CitiFinancial privacy policy describes the nature and extent of the information that will be collected. The privacy policy fulfills the principle of Notice of Existence and provides protection by informing the consumer what information is being collected, how it will be collected, and how it will be used.

In another example, Chase Bank received a rating of "3" in the principle of Notice of Existence for the privacy policy posted on their U.S. website due to the language contained in their policy, which is provided in Figure 6B.

Figure 6B: Chase Notice of Existence



Q. What information do you have about me?
A. To provide services and to help meet your needs, we collect information about you from various sources.

- We get information from your requests for our products or services. One example is income on loan applications.
- We get information about your transactions with us and with others. For example, we have your account balance information.
- We get information, such as your credit history, from credit bureaus.

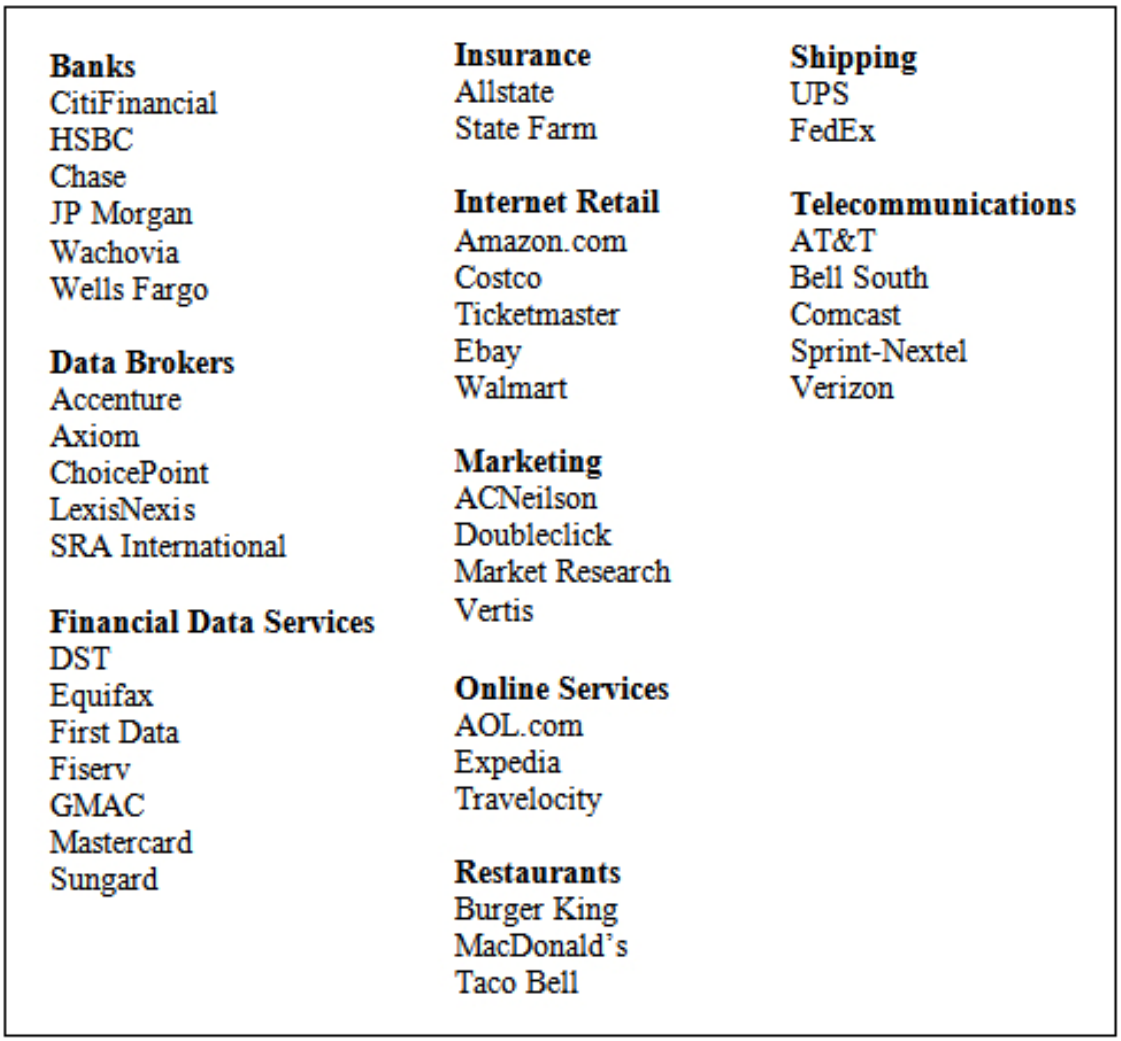
(http://www.chase.com/ccp/index.jsp?pg_name=ccpmapp/shared/assets/p..., 2007)

Chase received a lower score for the principle of Notice of Existence since the policy lists several ways in which consumer information is obtained, but the list is not exclusive. Chase does collect information from third parties, which are not obligated to abide by the same standards as Chase. In this example, Chase has provided notice that personal information is collected, but the extent of that collection is unclear, which limits assurance of protection. Furthermore, the privacy policy provided by Chase's U.S. website applies to all of the company's interactions with consumer information and is not limited to the website the way CitiFinancial's privacy policy was limited. The Chase rating of "3" for Notice of Existence applies to all of the company's interactions with consumers. This can be contrasted with the seemingly better CitiFinancial rating of "4" which only applies to the U.S. websites.

Company Selection

The list below details the industries and the sampling of companies from each that was studied for this thesis. The companies were chosen because they represent the largest companies in their respective industries (Fortune 500) and are considered leaders and trendsetters. Ratings will be measured by how closely the results align with the Fair Information Practices developed for this thesis.

Figure 6C: Company Selection



Banks
CitiFinancial
HSBC
Chase
JP Morgan
Wachovia
Wells Fargo

Data Brokers
Accenture
Axiom
ChoicePoint
LexisNexis
SRA International

Financial Data Services
DST
Equifax
First Data
Fiserv
GMAC
Mastercard
Sungard

Insurance
Allstate
State Farm

Internet Retail
Amazon.com
Costco
Ticketmaster
Ebay
Walmart

Marketing
ACNeilson
Doubleclick
Market Research
Vertis

Online Services
AOL.com
Expedia
Travelocity

Restaurants
Burger King
MacDonald's
Taco Bell

Shipping
UPS
FedEx

Telecommunications
AT&T
Bell South
Comcast
Sprint-Nextel
Verizon

Canadian Counterparts

Several of the companies selected for the privacy policy analysis also conduct business in Canada. Of the U.S. companies selected for analysis, sixty percent (60%) have separate privacy policies that applied to Canadian consumers. These Canadian privacy policies were also downloaded and analyzed along with their U.S. policies. U.S. companies that did not have Canadian privacy policy may not conduct business in

Canada or may not have a Canadian affiliate. In either case, since the consumer is limited to information available from the company's website, that is all that will be used for this analysis.

Upon initial review, the Canadian privacy policies are typically longer and provide more specific information and detail regarding their policy toward consumer data. Much of this additional detail can be attributed to language that addresses the requirements of PIPEDA and the Fair Information Principles. For example, McDonald's Canadian privacy policy goes so far as to identify and address each of the principles in distinct paragraphs describing how McDonald's policy satisfies the principle (http://www.mcdonalds.ca/en/privacy/privacyPrinciples.aspx, 2007).

Comparison and Analysis

Microsoft Excel and data analysis software SPSS were used to analyze the data in each of the company privacy policies. The policies were broken into sections, either continuous or fractured, that applied to each of the Fair Information Principles developed for this thesis. All company privacy policies received ratings for how it compared to each of the eight privacy principles. The scope of each privacy policy was also considered. Privacy policies were grouped as either having a scope limited to website transactions or being inclusive of all business transactions. Having a privacy policy of limited scope posted to the website may indicate that the company has an entirely different privacy policy for other transactions that may only be available to individuals after they become customers, if at all.

Data tables that include each privacy policy's ratings and scope are provided in Appendix B (U.S. Companies) and Appendix C (Canadian Companies). In summary, the analysis identified that almost sixty percent (60%) of U.S. privacy policies in this study had policies of limited scope, while the opposite is true in Canada. Over sixty six percent (66%) of the Canadian policies surveyed applied to all types of customer transactions (Figure 6D).

Figure 6D: Scope of Privacy Policy by Country

United States		**Canada**	
Web Only	59.5%	Web Only	33.3%
All Business	38.5%	All Business	66.6%

Further analysis of U.S. policies found large differences among industries. Industries, such as retail or online services, that conduct a lot of transaction through their websites were far more likely, eighty percent (80%) and one hundred percent (100%) respectively, to have privacy policies that encompassed all of their customer interaction. Another member of this group was the insurance industry. All four of the U.S. insurance companies surveyed had privacy policies that applied to all customer transactions.

On the other end of the spectrum, data-brokers, financial data providers, and restaurants were far more likely to have policies with limited scopes (Figure 6E). Privacy policies from these industries only provide information regarding how the company will handle the information it collects through its website. There is no indication of what information those companies might be collecting through other means, such as in-store business or phone business, and how they may be using it.

Figure 6E: Scope of Privacy Policy by Industry

Banks Web Only 22.2% (2 of 9) All Business 77.8% (7 of 9)	Marketing Web Only 75.0% (3 of 4) All Business 25.0% (1 of 4)
Data Brokers Web Only 100% (6 of 6) All Business 0% (0 of 6)	Online Services Web Only 0% (0 of 6) All Business 100% (6 of 6)
Financial Data Web Only 81.8% (9 of 11) All Business 18.2% (2 of 11)	Restaurants Web Only 100% (6 of 6) All Business 0% (6 of 6)
Insurance Web Only 0% (0 of 4) All Business 100% (4 of 4)	Shipping Web Only 75.0% (3 of 4) All Business 25.0% (1 of 4)
Retail Web Only 20.0% (2 of 10) All Business 80.0% (8 of 10	Telecommunications Web Only 33.3% (2 of 6) All Business 66.6% (4 of 6)

Privacy policies whose scope covered all customer transactions are more indicative of how a company will collect and handle customer data. Policies of limited scope only provide consumers a partial picture of the company's overall privacy policy. However, since consumers may only be able to access information which is available on a company's website, it is important to examine the trends among those policies surveyed, regardless of scope.

Several of the privacy principles stood out as the key indicators regarding how a policy compared overall. The first key principle was Consent. Companies that scored a 3 or 4 for the Consent principle were those that obtained some form of consumer consent prior to collecting their information. The consent had to be of the "opt-in" variety or a positive affirmation by the consumer that the collection was acceptable in order to

receive a rating of “3” or “4”. Only 16 of the 42 U.S. companies surveyed, or thirty eight percent (38%) scored a “3” or “4” for the Consent principle; compared to more than fifty four percent (54%) of Canadian companies that met the standard (Figure 6F).

Figure 6F: Consent by Country

United States		**Canada**	
Score of less than 3	59.5%	Score of less than 3	33.3%
Score of 3 or 4	38.5%	Score of 3 or 4	66.6%

Another key principle is the Limitation of Use. In order for a policy to receive a rating of “3” or “4” in association with the Limitation of Use principle should be clear at the time of collection what collected information will be used for. Collected information should not be used for a purpose other than that which it was collected.

The principle of Retention of Data seemed to be a failure point for company privacy policies on both sides of the border. Only 13 of 67, or less than twenty percent (20%), of all policies examined, both in the U.S. and Canadian addressed Retention of Data. Those 13 policies all addressed Retention of Data in a satisfactory manner, earning a “3” or “4”. The remaining companies failed to address the topic at all in their privacy policies (Figure 6G).

Figure 6G: Retention of Data by Country

United States		**Canada**	
Addressed Retention	14%	Addressed Retention	29%
Failed to Address Retention	86%	Failed to Address Retention	71%

Companies in both countries scored well when compared to the Access principle. According to the Access principle, consumers must have a way to access the information

that a company has about them. In several cases, companies scored well since their privacy policy was limited in scope to the website and consumers are able to create accounts on the company's websites where they are able to view some of their personal information. Unfortunately, these accounts do not necessarily provide consumers access to all of the information about them that may be stored by the company.

The principle of Accuracy was very closely linked to the Access principle. The same online user account that allows consumers access to their personal information, also allows them to update and correct information about themselves. In virtually all cases in both countries, a company that addresses both the Access and Accuracy principles in their privacy policy received the same score for both. The only exception came from American company, Equifax, who received a "4" for Access due to the extensive credit report that company provides customers, but received a "3" for Accuracy. Equifax received a "3" for Accuracy since consumers must appeal to the company in writing for changes to their credit report. All requests are subject to extensive review by Equifax. The score of "3" indicates Equifax's adherence to the principle but the privacy protections for the consumer can only be categorized as "moderate".

The Security principle did little to differentiate the policies of companies in the U.S. and Canada. The majority of companies in both countries addressed the principle in some form within their privacy policy. Any company that addressed security earned a "3" or "4", indicating their adherence to the idea that consumer data should be protected from misuse.

Chapter Summary

This chapter presented the privacy policy analysis part of this thesis. The privacy policy analysis was used to directly compare the privacy policies of companies in the United States and Canada and to compare those privacy policies against a set of Fair Information Principles. The purpose of the privacy policy analysis was to determine which country's companies had privacy policies that more closely aligned with the Fair Information Principles. The analysis demonstrated significant trends in the data.

The results indicated that Canadian companies are significantly more likely to have a privacy policy on their website that covered all of their customer interactions, instead of being limited to only those transactions that occurred through the website. Two-thirds of Canadian company privacy policies satisfied the Consent principle, while two-thirds of the U.S. company privacy policies did not. Companies in both countries were unlikely (86% in the U.S. and 71% in Canada) to satisfy the Retention principle or even address the issue in their privacy policy. Overall, Canadian companies scored significantly better in the comparison to the Fair Information Principles. This data can now be coupled with the Stakeholder Analysis in the next chapter to provide additional perspectives and answer the other research questions.

Chapter 7: Stakeholder Analysis

Stakeholder analysis "can be used to generate knowledge about the relevant actors so as to understand their behaviour, intentions, interrelations, agendas, interests, and the influence or resources they have brought – or could bring – to bear on decision-making processes (Brugha, 2000)." Privacy stakeholders are examined in both the United States and Canada in this chapter. In both countries, the stakeholders have been broken down into the following three categories:

- Government
- Industry
- Consumers

Each stakeholder group has an interest in how privacy policy is tailored in their respective countries. In some situations, the stakeholders of one country have a stake in the privacy policy decisions made by other countries, such as those when a company conducts business in both countries. This chapter will outline positions held by representatives of each stakeholder group. Examining the positions and statements of several group representatives will provide insight into what each stakeholder prefers regarding privacy policy.

U.S. Government

Each branch of the United States government is affected greatly by subtle changes in privacy laws and regulations. Privacy has become a key platform issue, and U.S. legislators must appeal to their constituent groups. Supreme Court decisions have hinged

on how the government defines privacy and how personal information is gathered as evidence.

Since 1974, the U.S. government has been regulated by the Privacy Act, which limits the collection and use of personally identifiable information by government agencies and representatives. The Privacy Act does not apply to companies and other non-governmental entities. As a result, government agencies often partner with private organizations to obtain the desired information they cannot collect on their own. In the event new legislation is passed to restrict non-governmental entities in the use of personally identifiable information, the government would be significantly impacted (Swecker, 2005). Some departments of the government, such as law enforcement and defense, may view additional privacy protection as an unwelcome hurdle.

On October 26, 2001, the `Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001' was signed into law (H.R.3162**)**. The PATRIOT ACT was part of the U.S. government's response to the terrorist attacks of September 11, 2001. The PATRIOT ACT establishes new rules regarding how law enforcement could pursue criminal suspects. Some groups, such as the American Civil Liberties Union, have claimed that the PATRIOT ACT was rushed into law, without a proper debate regarding its costs and benefits. The ACLU website claims the PATRIOT act contains:

> flaws that threaten your fundamental freedoms by giving the government the power to access to your medical records, tax records, information about the books you buy or borrow without probable cause, and the power to break into your home and conduct secret searches without telling you

for weeks, months, or indefinitely.

(http://www.aclu.org/safefree/resources/17343res20031114.html, 2003)

The USA PATRIOT ACT may have been passed only 45 days after the events of September 11th, but the powers it granted have been desired by law enforcement for decades prior. In the days following September 11th, the U.S. attorney general John Ashcroft instructed his subordinates to develop a package of desired authorities, "all that is necessary for law enforcement, within the bounds of the Constitution, to discharge the obligation to fight this war against terror (O'Harrow 2006, pg_15)."

The USA PATRIOT Act is a collection of law enforcement tools and national security exemptions that traditionally have been considered beyond the scope of the Constitution (Savage 2007, pg_82). Consumer protection organizations such as EPIC have argued these new tools are a dangerous threat to civil liberties and violate the privacy of innocent citizens. According to EPIC's website:

> [the USA PATRIOT Act] introduced a plethora of legislative changes which significantly increased the surveillance and investigative powers of law enforcement agencies in the United States. The Act did not, however, provide for the system of checks and balances that traditionally safeguards civil liberties in the face of such legislation
>
> (http://epic.org/privacy/terrorism/usapatriot/ 2005).

The debate between proponents and critics of the PATRIOT Act continues. Most recently, members of Congress have questioned FBI Director Robert Mueller after an inspector general report cited the Bureau for abusive use of so-called national security letters that allow the FBI to gather evidence without a court order (Schmitt, 2007). Much

of this evidence is gathered with the assistance of privacy organizations, such as telecommunications companies (Trotta, 2006).

One way agencies, such as the FBI, gather evidence is by purchasing information about individuals and their relationships from information resellers. During testimony before the United States Senate Committee on the Judiciary, FBI Assistant Director for Criminal Investigative Division, Chris Swecker, outlined the benefits of data resellers like ChoicePoint (Figure 7A).

Figure 7A: Testimony of Christ Swecker, FBI 2005

> An example of how Choicepoint can and has been used in analytical research can be seen in several of its search parameters. When the FBI has initiated an investigation, Choicpoint, through name and address information, can provide social security information on search projects. Once a social security number is available, analysts can enter this information into a new search parameter. These searches will produce all names that have ever been associated with the number. Many times, the production of these aliases can be used to run additional searches, providing even more potential leads for investigators to pursue. The automation of this multiple-source data, as with similar analytical engines, has dramatically reduced the amount of time and effort needed to include or exclude information.
>
> The Choicepoint search engines also provide the names of potential family relatives and co-habitant data for subjects and subject addresses. When used with other informational databases, including the Bureau's internal indices, potential and concrete links can be established between multiple facets of an investigation, and often assist analysts in developing links between previously unconnected investigations. As criminals and criminal organizations become more complex, need reasonable access to potential source of data and information that might afford them the opportunity to establish these types of links which are crucial to realizing the entire scope of an investigation.

Law enforcement relies heavily on data resellers like ChoicePoint to provide information. A Government Accountability Office (GAO) report reviewed four federal agencies: Justice, Homeland Security, State, and Social Security Administration. In fiscal year 2005 these four agencies alone reported a combined total of $30 million in obligations to data resellers for the purchase of personal information. Ninety one percent (91%) of this information was purchased for law enforcement and counter terrorism

purposes (Koontz, 2006). Not all U.S. federal agencies favor such practices. The FTC would like to see greater protection for consumer information as they stated in their 2000 report criticizing the current policy of industry self-regulation.

As previously stated, members of Congress, both Republican and Democrat are critical of the USA PATRIOT act due to the perceived privacy violations, such as warrant-less wiretaps. However, several members of Congress support enhanced privacy protection for consumers. For example, Senator Hillary Clinton personally supports specific legislation that would put consumers in charge of their personal information and provide them with the ability to hold both the government and private enterprise accountable for their actions and violations of privacy. In June 2006, Senator Clinton discussed her proposal in a speech before the American Constitution Society. The name of her proposal is the Privacy Rights and Oversight for Electronic and Commercial Transactions or the PROTECT Act, which contains what Senator Clinton calls a Privacy Bill of Rights (Clinton 2006). Proposals such as this are not unique. In fact, there are several proposals for new privacy legislation that have been put before both houses of Congress as discussed in the Chapter 2 literature review.

Companies

Any change to U.S. privacy policy would immediately impact companies and private organizations. Companies would be responsible for complying with any new rules, regulations, or laws. Companies currently have few restrictions on what data they can collect about individuals and what they can do with that data. Legislation that has been suggested by the FTC would curtail the amount of data that companies could collect

as well as limit what companies can do with that data, such as sharing it with a third party. Proposed legislation may also have a positive impact on customer trust and prove to be a competitive advantage as some have suggested (NYMITY 2006, pg_6).

One of the best ways to understand the views and opinions of companies is to review the testimony of industry representatives before Congress. In June 2000, the Chief Privacy Officer of DoubleClick testified before the Senate Committee on Commerce, Science, and Transportation regarding internet privacy, which is at the core of many consumer fears. DoubleClick is a leading internet advertising company that believes quality, targeted advertising is essential for keeping the internet free. They argue strongly for the continued ability of companies to use customer transactional data for advertising purposes. It is their belief that "marketing data" is not a threat to consumer privacy. At the same time, DoubleClick also advocates a policy of consumer education regarding privacy and belongs to the Network Advertising Initiative to further educate consumers. DoubleClick believes consumers have a right to know what types of data are being used by advertising companies and have a right to control the use of that data by opting out of having data collected (DoubleClick, 2000).

While companies like DoubleClick say they put extensive effort into protecting consumer privacy, other testimony demonstrates a desire to keep customers satisfied by minimizing the impact on consumer conveniences. In September 2006, the vice president of Corporate Transactions and Business Law for Sprint-Nextel, Charles Wunsch, testified before an Oversight and Investigations subcommittee of the House, that providing consumer protection is not difficult. The challenge comes in "balancing protection and the consumer's desire for convenience (Wunsch, 2006)."

Stuart Pratt is the President and CEO of the Consumer Data Industry Association (CDIA). “CDIA represents the consumer credit reporting information industry before state and federal legislators. It also represents the industry before the media in consumer credit reporting matters (cdiaonline.org, 2007).” In April 2006, Stuart Pratt testified before the Joint Hearing subcommittee on Commercial and Administrative Law and the subcommittee on the Constitution of the Committee on the Judiciary House of Representatives. Pratt’s testimony focused on the benefits of the services provided by the information industry. Pratt also criticizes previous testimony and government reports on the subject of privacy for trying to apply the Fair Information Practices as a “one-size-fits-all yardstick”. Pratt argues that even within the information industry, there are several different business models serving different purposes, and that it would be inappropriate to regulate them all in the same manner” (Pratt, 2006).

Each industry views privacy differently and different industry advocates present varying cases for why their businesses are valuable to consumers or government. It is; however, clear that many companies and industry representatives object to the outright application of the Fair Information Practices. Some of the primary reasons are:

- Lack of flexibility for customer service
- Different information should be handled in a variety of ways
- Consumer access can corrupt otherwise accurate data, by allowing them to delete embarrassing or inconvenient information from their profiles

Consumers

The personal information of consumers is sought after by both companies and government. Controlling that desire for information would be the goal of any new policy. Polls indicate that U.S. consumers are very concerned about their privacy and yet are unaware of the actual protection or lack thereof, which they are entitled to under current law (http://epic.org/privacy/survey/, 2008). The FTC, EPIC, and Annenberg report in Chapter 2 all spoke to a lack of understanding by the general public and the concern they have for how companies protect their personal information.

In February 2005, information reseller ChoicePoint began notifying more than 100,000 U.S. consumers that their personal information had been inadvertently sold to fraudulent businesses and that they may become victims of criminal activity as a result. More than 700 notified individuals later reported having their addresses changed. Identity thieves typically change a target's address in order to obtain credit card offers or other mail. Letters to victims from ChoicePoint said, "We have reason to believe your personal information may have been obtained by unauthorized third parties, and we deeply regret any inconvenience this event may cause you (O'Harrow WashPost, 2005)." These notifications first were sent to residents in California, which is the only state in the United States that requires companies to notify consumers when their information is stolen or obtained inappropriately. Consumers outside of California were notified once the extent of the breach was discovered by the media (O'Harrow WashPost, 2005).

Unhappy consumers are not able to take their business elsewhere, because ChoicePoint collects information about individuals through a variety of means which seldom include direct solicitation. ChoicePoint maintains databases with billions of

records about nearly every adult in America, including credit reports and criminal records. It has acquired more than 50 other information companies since its inception. Like other information resellers, ChoicePoint routinely sells their information to police, lawyers, reporters, intelligence and homeland security officials as well as credit agencies, debt collectors, insurance companies, and check-cashing businesses (O'Harrow WashPost, 2005).

In the aftermath of the 2005 ordeal ChoicePoint is considering "fundamental changes" in security procedures and customer authentication. ChoicePoint spokesman James Lee stated, "We're not to blame, but we're taking responsibility -- The people committing the fraud were smarter and quicker than we were (O'Harrow WashPost, 2005)."

Marc Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC), stated the case raises important questions regarding who is responsible when companies are duped into releasing data. "Companies such as ChoicePoint are operating with too little oversight," he said (CNN, 2005).

Consumer concerns cause groups such as the Center for Democracy and Technology (CDT) to advocate for stronger protections and increased oversight. CDT's mission is to "conceptualize, develop, and implement public policies to preserve and enhance free expression, privacy, open access, and other democratic values" on the Internet (CDT.org, 2007). In testimony before the U.S. Senate Committee on the Judiciary, CDT Executive Director James Dempsey said, "While data brokers provide important services to the government and the private sector, they also raise a host of

privacy issues and concerns about the security of this information." Mr. Dempsey went on to say that

> Even legitimate uses of personal data can result in harm to individuals. For instance, individuals can suffer adverse consequences when data brokers sell inaccurate or incomplete information that result in the loss of employment opportunities. In the context of government use of personal information, adverse consequences could include being suspected of criminal or terrorist activity. (Dempsey, 2005)

During his testimony Dempsey mentions a book written by Robert O'Harrow titled *No Place to Hide*. In his book O'Harrow cites several cases, in which legitimate uses of data gathering and reselling have resulted in false arrests, harassment, and financial devastation for those unfortunate enough to have their electronic profiles mixed up by incorrect information.

Canada's Stakeholders

The previous section provided a look at the positions and viewpoints of the three major stakeholders in the U.S. Each stakeholder has their own goals and concerns regarding changes to U.S. privacy laws and regulations. In Canada, those same stakeholders have spent the last several years adjusting to PIPEDA and the changes it made to Canadian privacy policy. This section will examine the reactions of each group as they experience and implement the changes brought about by PIPEDA.

The U.S government is regulated by the Privacy Act, not PIPEDA, but the government is responsible for enforcing the rules outlined in PIPEDA, even when those laws may prevent the government from using private organizations to assist it in information gathering and processing similar to the U.S. government. While others parts of the government, like the Supreme Court, have called for strengthening the law and the powers given to the Privacy Commissioner (Geist, 2006).

The second group impacted by PIPEDA is the private organizations and industries governed by PIPEDA's rules. Some have argued that laws like PIPEDA cause companies and organizations to incur unnecessary financial costs that ultimately affect the economy. Some organizations have chosen to view compliance with PIPEDA as a competitive advantage that attracts customers; while others view it as a burden (Observer, 2003). The final group directly impacted by PIPEDA is the citizens of Canada whose personal information is being protected by the law. Polls show Canada's population is overwhelmingly in favor of privacy protections provided by PIPEDA. The subsequent section will take a closer look at how each of these three groups are reacting to PIPEDA.

Government

September 11th had a significant impact on the minds of Canadians, much the same way it impacted Americans. The Canadian Parliament passed the Anti-Terrorism Act in December 2001; only two months after U.S. President Bush signed the USA PATRIOT Act. The Anti-Terrorism Act was part of the Canadian Parliament's Ant-Terror initiative, launched after September 11th. Section 7 of the Anti-Terrorism Act modifies clauses in PIPEDA to include exemptions for evidence being gathered for a

criminal case and block the Privacy Commissioner from releasing any findings or discussing these types of cases publicly. These modifications to PIPEDA show the Canadian governments dissatisfaction with the limitations PIPEDA imposed on law enforcement.

In 2002, Canadian Parliament passed The Public Safety Act, which went even further than the Anti-Terrorism Act in its modifications of PIPEDA. The changes were summarized by Murray Long in an interview with NYMITY in July of 2004.

> There are three amendments, all in section 7 of the Act, which lays out the exceptions to consent. The first is that organizations can now collect personal information without an individual's knowledge or consent where the collection is for the purpose of making a subsequent disclosure as required by law. Previously, organizations could disclose personal information without consent where required by law, but there was no such exception for collection. Consent had to be obtained, except where the legal purposes had to do with an investigation.
>
> The second change is that PIPEDA now permits an organization to collect new information about an individual where either CSIS or the RCMP, the two agencies responsible for national security, make a request for the collection and the data relates to a national security interest. The third change is that an organization can now also collect new personal information, on its own recognizance, in the same circumstances – i.e. wherever the organization suspects the information might be relevant to

> national security interests, and the organization intends to subsequently disclose it either to a security agency or to an industry investigative body (Long NYMITY, 2004).

The above modifications were described and discussed by the Privacy Commissioner and described in a speech in 2004 as blurring the line between the public and private sectors. Ms. Stoddart's concerns stemmed from the amendments that allow private firms to collect information on behalf of national security agencies (Stoddart, 2006). Murray Long, in his 2004 NYMITY interview, also described these amendments as corrosive to transparency and cites the amendments that allow commercial enterprises to actively search out information that it will then disclose to a national security agency.

In reality, the amendments contained in both the Anti-Terrorism Act and the Public Safety Act do little more than what was already allowed under PIPEDA. PIPEDA already provided commercial organizations the right to disclose information to law enforcement that the organization discovers in the course of doing business. While the amendments mentioned above do permit organizations to expand their search beyond what they may encounter during the course of business, they must disclose this information to the authorities promptly after it is collected. It also does not provide them with the right to maintain that information after it has been disclosed.

Industry

NYMITY is a leading privacy research firm in Canada. Their clients include privacy officers, lawyers with privacy practices, privacy consultants and privacy

commissioner's offices across Canada. NYMITY routinely interviews industry executives and agency leaders across Canada regarding their privacy concerns and issues. A majority of these interviews include the interviewee's opinions on the impact of PIPEDA. One such interview was with David Elder, the Assistant General Counsel for Bell Canada, Canada's leading communication company (2006). The Bell Canada executive outlined his top ten lessons learned from 3 years of operating under PIPEDA.

Counting down from 10 to 1, the executive's first lesson learned involved subcontracting work that involves the personal data of individuals. This could be subcontracting work to a data processing center. Elder recommended not simply forcing (via contract) third parties to abide by all aspects of your own companies privacy policy, or try to bind them to PIPEDA if they are not already bound. Mr. Elder suggests that a "one size fits all" approach to privacy is the wrong way to go. He suggests that companies tailor their contract to fit the situation and the data that is being shared. This suggests that companies (at least Bell Canada) have found it useful or less troublesome to make privacy a crucial part of day-to-day business rather than attempting to relegate it to a standard clause in their contracts (Elder NYMITY, 2006).

When it comes time to engage the inevitable customer requests for information, Mr. Elder again recommends a custom approach. He suggests that providing more information is better than providing too little. Give the customer/requester as much information as possible and where it is necessary to redact some information provide the customer/request with detailed reasoning of the type of data being redacted and why it is being withheld. These suggestions to industry indicate it is easier/prudent for companies to show their customers a certain level of respect. In the long run, it saves the company

from having to deal with follow-up inquiries, formal complaints, or lawsuits (Elder NYMITY, 2006).

Mr. Elder further suggests that creating a clear and short privacy policy is preferable to trying to confuse customers/clients with a long and complex one. Ongoing employee training also is highlighted as crucial to success and having designated privacy personnel whenever possible is highly recommended. His final and more important suggestion is, "Don't circle the wagons." Trying to stonewall customers/requesters or even the privacy commissioner is the least helpful avenue. He recommends openness, and establishing a good working relationship with the privacy commissioner (Elder NYMITY, 2006).

These statements from a leading counsel for one of the biggest companies in Canada suggest a very positive role being played by industry in Canada's privacy efforts. Mr. Elder went so far as to indicate that privacy rules had made it easier to do business since the laws had established trust and predictability where there used to be very little.

NYMITY recently published their 2006 Trends in Transparency. The report is, "released in conjunction with the Canadian Marketing Association (CMA) to raise industry awareness about the importance of privacy notice transparency, and to highlight best practices adopted by many leading organizations serving the Canadian marketplace NYMITY 2006)." NYMITY outlines the status of the largest companies (by revenue) in 8 different industries (Figure 7B).

Figure 7B: Trends in Transparency (2006) Industry Selection

- Insurance
- Financial Services
- Banks
- Telecommunication
- Retail
- Media
- Consumer Services
- Business Services

These industries interact with the public on a daily basis as part of their business operations. Overall, NYMITY identifies a positive trend from their results. Industry is aware of privacy concerns and they are responding in a positive fashion. Most have followed the recommendations of the Privacy Commissioner or the CMA in implementing their privacy policies in a transparent or open fashion. The NYMITY report provides evidence that some industries, on average, are doing better than others at protecting consumer privacy. For example, the banking industry demonstrated the "highest level of transparency related to the handling of personal information." NYMITY explains that the banking industry is considered a Federal Work under PIPEDA and thus fell under PIPEDA's requirements years before other industries. This head start has given the banking industry more time to comply and to improve their practices (NYMITY, 2006).

The fact that the industries that have been required to comply with PIPEDA the longest amount of time are doing a better job of being transparent and sensitive to personal information demonstrates positive results. The banking industry has found that customers as well as other businesses are more willing to work with them when their privacy policies are transparent and sufficiently protective of personal information. Their

hard work and progress made on privacy matters has resulted in a competitive advantage according to NYMITY's findings (NYMITY, 2006).

Reading the report begs the question, "do the companies that earn recognition for success under PIPEDA demonstrate the same level of care for privacy in other jurisdictions?" The answer is; *it depends.* Some companies, such as Ticketmaster, had identical privacy policies for both their United States offices and their Canadian offices. Other companies such as Equifax (a credit agency), specifically label their U.S. privacy policy as 'U.S. Only', and have a very different policy for their offices/customers in Canada. In fact, the "U.S. Only" policy only covers those transactions that occur online through one the U.S. based Equifax websites. The privacy policy that Equifax uses in Canada is an award winning policy (NYMITY, 2006) and covers the entirety of Equifax's business in Canada.

Equifax is not only capable of meeting the requirements of PIPEDA for its Canadian offices, but it excels; while at the same time being far less transparent or informative in the U.S. In a brief review of the companies in the NYMITY report, it was apparent that several companies have different standards for privacy policy in Canada than they do in the United States. eBay and Wal-mart were both recognized in NYMITY's report, but both have rather different privacy policies in the U.S. where nothing like PIPEDA exists.

Consumers

There are three parties specifically addressed in Canada's privacy legislation. This research has already addressed U.S. and Canadian government. Second, this

research examined U.S. company positions and the positions of the Canadian organizations regulated by PIPEDA. The last comparison to make is that of U.S. and Canadian consumers.

Opinion polls are a convenient way to gauge public opinion. Pollsters use their skills to forecast elections, the economy, and new commercial products. While public opinion polls overwhelmingly show that the general Canadian public is in favor of privacy legislation, this research examined another, less quantitative source of public opinion. In order to gauge the public perception of PIPEDA, a sample of 10 editorials were examined. The editorials were pulled randomly from a LexisNexis search of the last five years and from a variety of publications both prior to and after the passage of PIPEDA. The expectation is that these opinions pieces may highlight concerns and opinions that may have been glossed over in polling alone. The article samples came from the following publications and were judged to have either a positive or negative view of PIPEDA. A summary of the results is provided in Figure 7C.

Figure 7C: Results of Canadian Editorials Regarding PIPEDA

Publication	**General View of PIPEDA**	
	Positive	Negative
London Free Press (Ontario)	X	
London Free Press (Ontario)	X	
The Leader-Post (Saskatchewan)	X	
Windsor Star (Ontario)	X	
Peterborough Examiner (Ontario)	X	
ComputerWorld Canada	X	
The Toronto Star (Ontario)	X	
Pembroke Observer (Ontario)		X
Pembroke Observer (Ontario)	X	
Edmonton Sun (Alberta)	X	

Only one of the editorial pieces reviewed demonstrated any negative views of privacy legislation or PIPEDA in general. Written prior to PIPEDA taking full effect, the unknown author saw PIPEDA as an unnecessary and crippling burden placed on small businesses in Canada. He charged that PIPEDA would force small businesses to hire consultants and lawyers to navigate the complex nature of the law. He also charged that these new impediments to efficiency would slow down business and cause cost over-runs that would be especially damaging to small businesses (Observer, Oct 30 2003).

Oddly enough, another sample was a write-in to the same publication only 2 weeks later. This author, Mark Kutschke, chastised the publication for running the critical piece and accused the author of having a vested interest in the selling of lists of names and addresses. He then goes on to praise PIPEDA and the efforts of the Canadian government to protect individuals from the threats of a modern information-driven world (Observer Nov 14 2003).

Overall the editorials cast PIPEDA in a positive light. Four of the editorials (Jacobs, 2003; Beres, 2003; Samel, 2003; Nantaris, 2005) went so far as to call upon companies and government agencies/employees, especially those in management positions, to do a better job of understanding the law and implementing changes to their policies and procedures. One writer said:

> Information security goes far beyond the use of fire walls and virus scanners. It involves the senior management's commitment to governing the proper collection, use, protection, and disposal of information by their organization (Nantaris, 2005).

It seems apparent that the Canadian population, or at least those participating in and aware of the issues, are supportive of the Parliament's privacy legislation and the efforts of the Privacy Commissioner to move it forward. The only major concern among private citizens is that although companies write policies, they sometimes fail to disseminate them to their employees, or fail to act appropriately. One writer questioned how many companies would have to be dragged into court before the rest got the picture (Beres, 2003). Canadians are concerned about their privacy and they believe it to be a very serious issue.

Chapter Summary

This section has outlined the views and positions of the three different stakeholder groups interested in privacy legislation. Each stakeholder group is diverse even among itself, but there are major themes that have been identified. The federal government has several separate agencies with sometimes very different agendas. A balance must be achieved in privacy policy that allows law enforcement to pursue criminals and national security threats, without compromising the rights of its citizens or the trust in the market that remains critical to a thriving economy.

Industry is resistant to further enforcement of privacy policy objectives due to the perceived threat to flexibility. Industry is highly dependent on its ability to satisfy customers. Industry representatives have cited an ongoing balance between the desires of the customer to have convenient and quick services and the demands of the customer for protection of their data. Industry feels that additional enforcement from the government will tip that balance unfavorably.

Consumers and consumer interest groups are driven by a variety of needs and desires. It is their mixed needs that lead industry to fear additional restrictions and for some government agencies to pursue those same restrictions. Consumers must have a certain degree of confidence in their ability to participate in the marketplace without losing control of their personal information. Without such confidence, consumers will shy away from new technologies and new markets until their confidence is restored. Conversely, consumers also demand convenience and speedy service that can be at odds with safe and secure transactions. A balance must be found among these competing needs and desires.

Chapter 8: Discussion and Findings

This chapter will include a discussion of the research results in the form of case studies and a breakdown of findings to each of the research questions. The goal of this chapter will be to answer the research questions using the results collected. The case studies examine real world examples of three companies and their privacy policies. Then, each of the research questions is broken down into their elements for discussion and findings. The chapter will conclude with a summary of the findings and an introduction to the recommendations resulting from this research, the limitations of this work and next steps for future research.

Case Studies

This section will outline three case studies for discussion. The first case is HSBC, which was selected as a member of the banking industry. HSBC's U.S. privacy policy is very different from their Canadian privacy policy. The second case is of ChoicePoint, a company selected as a member of the data brokering industry. ChoicePoint did not have a separate website or privacy policy for Canadian consumers, and their privacy policy is limited in scope to their website. This limited scope allows ChoicePoint to produce an attractive privacy policy that scored well compared to the privacy principles of this study. Finally this section examines Wal-Mart. A member of the retail industry, Wal-Mart has separate privacy policies in both countries, each covering all consumer transactions. These case studies provide a real world look at how privacy policy is implemented in the U.S. and Canada.

HSBC

HSBC was selected for the privacy policy analysis as a member of the banking industry. HSBC has a different privacy policy for its Canadian customer than it does for those in the U.S. Figure 8A depicts the scores received by each HSBC privacy policy as compared to the privacy principles used for this research.

Figure 8A: HSBC Content Analysis Ratings

Principles	**HSBC U.S.**	**HSBC Canada**
Notice of Existence	4	3
Consent to Collection	0	4
Limitation of Collection	4	4
Limitation of Use	3	4
Retention of Data	0	0
Access to Data	0	4
Accuracy of Data	0	4
Security of Data	4	4

The data indicates that HSBC's U.S. privacy policy failed to address the principles of consent, retention, access and accuracy, but scored well with the remaining principles. What this data does not show is that HSBC's U.S. policy is limited in scope to only those customer interactions on its website. The U.S. policy failed to address several key privacy principles and it is unknown how HSBC would have scored had their full privacy policy been available. Potential HSBC customers are not able to inform themselves of HSBC's privacy practices through the company website.

By contrast, the privacy policy HSBC provides Canadian consumers applies to all types of consumer transactions and compares favorably with the privacy principles.

HSBC's U.S. privacy policy is one page in length and does little more than assure the reader that at HSBC they, "respect your privacy and value your trust." Conversely, the privacy policy provided to Canadian consumers contains detailed information to consumers in a Q&A format. It also includes contact information for the company's privacy officer and instructions that inform consumers how they can change how HSBC handles their individual personal information.

The HSBC case study highlights the stark policy contrast that can be observed within the same company simply by crossing the border. However, the comparison of information uses showed no difference between the policies. The more protective Canadian policy did nothing to impact HSBC's ability to conduct business with it's customers. In fact, the Canadian privacy policy ends with the following statement:

> If you do refuse or withdraw your consent to any of the above uses of your personal information, it will not affect your eligibility for credit or other products or services (http://www.hsbc.ca/code/tools/site/, 2007).

ChoicePoint

ChoicePoint presented an interesting case. ChoicePoint's privacy page showcases the TRUSTe certification for privacy. The privacy symbol indicates that ChoicePoint has met certain benchmarks, established by TRUSTe, for privacy security on their website. The TRUSTe symbol only applies to the company's website and does not necessarily indicate that ChoicePoint's other business operations meet the TRUSTe privacy standards.

As described in the Annenberg report, consumers are often confused by the lack of common language used in privacy policies (Turow, 2006). ChoicePoint's site indicates that their online policy "reflects and implements – in an online setting – our corporate privacy principles (http://www.choicepoint.com/privacy.html, 2007)." This language might lead a consumer to believe that the online policy is much the same as the policy implemented for all ChoicePoint's consumer interactions. ChoicePoint even goes so far as to indicate it promotes fair information practices. In reality, ChoicePoint is in the business of collecting consumer information from third parties and then selling that information to its governmental and corporate customers (Swecker, 2005). These transactions occur without customer knowledge or consent. Some transactions received significant press coverage when ChoicePoint was required under California law to notify consumers that their information had been sold to identity thieves accidentally. ChoicePoint estimates thieves were able to purchase personal information on over 140,000 Americans before they were discovered. ChoicePoint maintains files on nearly every American and sells that information to a variety of customers (CNN, 2005). It is difficult to know what types of information may have been compromised; ChoicePoint does not provide a way for individuals to request that type of information, unless the information was provided to ChoicePoint through their website (http://www.choicepoint.com/privacy.html, 2007). The Content Analysis research gave ChoicePoint positive scores in the comparison to the privacy principles (Figure 8B). However, when that information is compared with the results of the stakeholder analysis and the literature review, it is clear that ChoicePoint's online privacy policy is not indicative of their business practices in general.

Figure 8B: ChoicePoint Content Analysis Ratings

Principles	ChoicePoint
Notice of Existence	4
Consent to Collection	3
Limitation of Collection	4
Limitation of Use	3
Retention of Data	3
Access to Data	3
Accuracy of Data	3
Security of Data	3

Wal-Mart

Wal-Mart has two different privacy policies for U.S. customers and for Canadian customers, but neither policy is of limited scope. The policies for each country cover all customer transactions and both received positive scores as indicated in Figure 8C.

Figure 8C: Wal-Mart Content Analysis Ratings

Principles	Wal-Mart US	Wal-Mart Canada
Notice of Existence	4	3
Consent to Collection	3	3
Limitation of Collection	4	3
Limitation of Use	3	4
Retention of Data	0	4
Access to Data	4	4
Accuracy of Data	4	4
Security of Data	4	4

While the Canadian policy received higher scores in several of the principle areas, both policies provide significant protection to consumers and generally adhere to the Fair Information Principles. Although there were some companies that had the same identical privacy policy for both counties (FirstData, MasterCard, AT&T), Wal-Mart had differing

policies that still provided similar levels of protection without limiting the scope to their website.

Wal-Mart provides an excellent case study due to the size and scope of their business. Their retail sales occur both online and in stores, and they have locations in 15 different countries worldwide (walmartstores.com, 2007). Wal-Mart stores include pharmacy services that give them access to consumer health and medical information, as well as access to vast amounts of consumer purchasing information. Wal-Mart's privacy policies demonstrate that a large profitable company is able to maintain high standards of individual privacy.

Answering the Research Questions

This section will review the research questions outlined in Chapter 4 and present the research findings relative to each question that were obtained from the privacy policy content analysis and the stakeholder analysis.

Question 1 - Is Canada's Privacy Policy (PIPEDA) more effective than U.S. policy of industry self-regulation at achieving the Fair Information Principles in company privacy policies?

The privacy policy content analysis clearly shows a significant difference between the privacy policies of U.S. companies and their Canadian counterparts. The difference is particularly striking given that many of the companies conducted business in both countries, yet they had different privacy policies in each.

While the limited scope does confuse the results by leaving much unknown, it is apparent that Canadian consumers receive a better picture of how Canadian companies use and manage their information and what consumer rights are. Even the issue of consent seems to be experiencing significant progress under the Canadian system, despite being one of the biggest challenges to the Canada's privacy policy (NYMITY, 2006). Nearly sixty percent (60%) of U.S. policies in the study received less than a satisfactory score on the issue of consent, while Canadian companies' privacy policies received passing scores more than two-thirds of the time. It is clear that PIPEDA has brought Canadian companies' privacy policies significantly more in line with what the FTC would like to accomplish in the U.S. The data collected for this research provides a clear answer to the first research question. Canada's privacy policy (PIPEDA) is more effective than U.S. privacy policy (industry self-regulation) in achieving the Fair Information Principles.

Question 2 - Should PIPEDA be used as a model for future U.S. privacy policy, and if so what lessons can be learned from its nearly seven year history?

The success of PIPEDA demonstrated in this research creates a useful model for changes to U.S. privacy policy. The privacy policy content analysis demonstrates how much closer PIPEDA has brought Canadian companies to the Fair Information Principles in less than a decade. Unfortunately, the stakeholder analysis indicates a significant amount of resistance to changing U.S. law in a way that would make the privacy principles enforceable. The company testimonies reviewed in Chapter 2, revealed strong

objections to additional restrictions on company behavior. National security and law enforcement needs must be given consideration as well.

PIPEDA created a new government agency under the Privacy Commissioner and such changes would most likely be viewed as a duplication of existing bureaucracy in the United States. The FTC is already charged with the protection of the U.S. consumer. PIPEDA should be closely examined for its successes in Canada, but its difficulties and the resistance such changes are facing in the U.S. must be considered in order to provide the most effective solution for the U.S. stakeholders. The issues of scope, consent, and industry business models must all be considered prior to changing the U.S. privacy policy for industry. Policy changes similar to PIPEDA would have to be adapted to U.S. needs; although it should be clear that these needs are not due to differences in the U.S. and Canadian markets, but differences in existing government infrastructure and differences in the roles played by stakeholders.

Question 3 - Who are the critical stakeholders concerned with U.S. privacy policy and how do their positions impact future policy changes?

The three major stakeholders identified as key to the development and implementations of U.S. privacy policy are the federal government, industry, and consumers. These broad categories of stakeholders were chosen because there are corresponding stakeholder groups that are easily identified in the Canadian system and are subsequently used as a point of comparison. Governments in both countries are responsible for creating the laws and regulations governing privacy policy. Industries are

responsible for implementing the privacy policy in their day-to-day operations. The consumers are the primary beneficiaries of the privacy protections. These three groups only represent broad categories of stakeholder and dissenting opinions do exist within each stakeholder group.

Government

The U.S. government creates and enforces federal privacy policy, but there are differing goals and objectives concerning privacy policy among the various branches and agencies. Within the executive branch, different agencies have varying missions and objectives. The security and law enforcement agencies, like the FBI and military, rely on data sources and data collection for their enforcement and national security roles. Restrictive privacy policies can create obstacles to their collection and processing of personal information.

The Federal Trade Commission (FTC) is charged with protecting consumers, and as such advocates stronger privacy protections for consumers (ftc.gov, 2007). This position can put them at odds with law enforcement and national security agencies because the enforcement and security agencies often desire access to consumer personal information. In Canada, there is a similar struggle between the national security agencies and the Privacy Commissioner. Amendments to PIPEDA have provided exceptions to the law for national security and law enforcement that the Privacy Commissioner has publicly decried as unnecessary and dangerous (Canadian Press, 2006).

The legislative branch of the U.S. government consists of representatives that create laws. These representatives have positions and objectives based on the

relationship they have with their constituencies, which include the average consumer in their district or state, as well as special interest groups (Clinton, 2006; Biden, 2006). The priorities of the consumer and special interest groups are subject to changes, as was seen after the events of 9/11. Laws such as the PATRIOT Act, which gave more freedom to law enforcement and national security agencies, were quickly passed with little consideration for the privacy implications (Swire, 2002; Swire, 2006).

In Canada, the same is true and members of the Canadian Parliament are subject to the same pressures from similar constituent groups. The amendments to PIPEDA were passed shortly after the PATRIOT Act and also provide additional freedoms for law enforcement and national security agencies (Canadian Press, 2006). However, the Canadian Parliament was able to pass PIPEDA in 2000, while the U.S. Congress has been unable to pass privacy legislation that even remotely resembles the protections offered by PIPEDA.

Industry

The term 'industry' encompasses several different types of companies with a variety of missions and business models. Not every business will view federal privacy policy the same way. Most businesses seldom interact with consumer's personal information and have no desire to collect it. There are however, several business models that rely heavily on the collection of consumer's personal information where more restrictive privacy policies can have potentially debilitating effects on their revenue. Companies, such as those reviewed in the privacy policy content analysis, interact with consumer personal information on a daily basis and regularly store that information for

future use. Those businesses categorized as data brokers make their money by selling that consumer information to other businesses and to the government.

Industries collect consumer information because it provides numerous competitive advantages. More specific information about consumers allows for higher-quality and more targeted advertising. It also allows them to provide more convenient services that are tailored to the customer's needs and desires. For example, by understanding a customers purchasing history, Amazon.com is able to make recommendations to the customer based on their likes and dislikes. They are also able to offer additional conveniences like discounts on faster shipping to those customers who frequently expedite their purchases (amazon.com, 2007).

Industry has a strong motivation to influence the outcome of any changes to federal privacy policy and several industries spend significant amounts of money on lobbying and campaign donations to candidates that will work in their favor (opensecrets.com, 2007). It is clear through reviewing the testimony of industry representatives, that they favor less restrictive rules on privacy and strongly advocate for a policy of industry self regulation, which has been shown to be ineffective with regards to the standards outlined by the FTC (Wunsch, 2006; Faley, 1999; Curling, 2005; Turow, 2006).

In Canada, the situation is very similar. Canadian industry has the same motivating factors and expressed the same concerns regarding increases to costs and loss of competitive advantage (The Observer, Oct 30, 2003). After PIPEDA was passed however, industry groups such as NYMITY have demonstrated the competitive

advantages of providing customers with increased privacy protection and the trust it fosters between the consumer and the business (Elder, 2006).

Industry would prefer to have a privacy policy of self-regulation and optional guidelines. Their lobbying efforts describe their aversion to government intervention and the potential loss of flexibility and competitive advantage. However, several of these same companies maintain divisions within Canada and operate successfully under PIPEDA's regulations. Most of these businesses have even won awards from organizations such as NYMITY for their exceptional privacy policies and consumer protections provided by their Canadian divisions (NYMITY, 2006).

Consumers

Consumers also have competing values. Some are strong advocates for consumer protections and some are far more concerned about the conveniences and protections provided by the collection of their personal information. In general, however, consumers are wary of industry and government when it comes to the collection of their personal information. Polls conducted over the last several years indicate two thirds of respondents are worried about the uses of their personal information by both industry and government. Consumers are especially concerned with the current policy of self-regulation and believe it to be inadequate to protect their privacy (http://epic.org/privacy/survey/, 2008).

Industry points to customer pickiness about convenience and service. However, laws like PIPEDA require all companies to provide the same level of protection, which saves the company from having to compete with rival companies for a customer service

advantage. In congressional testimony, representatives from Sprint-Nextel stated that, "Providing additional protection for customer information is not difficult: the difficult part is balancing protection and the customer's desire for convenience" (Wunsch, 2006). The current federal privacy policy of self regulation can leave responsible companies at the mercy of those who have far less concern about consumer's privacy. The Annenberg Report of 2006 previously demonstrated that consumers are unaware of the severity of the threat to their privacy. Thus, without the knowledge to discern between those companies protecting their information and those abusing it, consumers may choose to give their business to those companies offering the greatest convenience. In this case the market is failing to accurately inform consumers and it is the responsible companies that suffer.

In Canada, it may be too soon to discern if PIPEDA has corrected the failure of the market to inform consumers. However, the Canadian Privacy Commissioner resolves hundreds of cases each year which result in consumer's rights being protected and companies complying with the new law without the need for litigation.

Each group (government, industry, consumers) has a role to play in shaping any changes, or lack thereof, to U.S. privacy policy. Currently the federal government will continue to pursue national security and enforcement, often at the expense of consumer privacy. However, the FTC does have the power to create and enforce regulations that would provide the necessary protections. It is possible for the FTC to move forward with new regulations over the objections of other executive agencies.

Industry will continue to pursue a policy of self-regulation since it provides the maximum flexibility and provides the minimum liability. Industry will continue to

provide additional technological protections against identity theft as legal liability increases.

Consumers remain distrustful of both industry and government and desire additional protections. Consumers may take individual steps, such as installing privacy software on their computers, to protect their privacy but without sufficient knowledge to adequately do so. Policy windows can emerge as high profile cases of privacy and abuse of personal information appear in the media. These policy windows increase the public concern and desire for additional legal protections. These concerns have the potential to drive legislative change, by putting pressure on U.S. representatives to enact meaningful change.

Question 4 - Would a change [to in] policy similar to PIPEDA impact various U.S. industries differently and if so are those impacts significant enough to be considered when adopting future privacy policy?

The privacy policy analysis indicates differences among industries; however, it is difficult to draw conclusions due to the significant number of U.S. company privacy policies of limited scope. Nearly sixty percent (60%) of the U.S. company privacy policies examined were limited in scope to consumer interactions with the company website. Without access to additional information, it is difficult to draw a solid conclusion.

The stakeholder analysis does reveal that during congressional testimony, data broker companies and marketing companies are more aggressive in their efforts to

maintain the status quo of U.S. privacy policy. Representatives of ChoicePoint, DoubleClick, and the Direct Marketing Association strongly discouraged government involvement in privacy protection; instead encouraging the government to continue with a policy of industry self-regulation.

For many industries the difficulty seems to be the issues of consent, both to collection and sharing of their collected information. This is also true among Canadian companies as well. Companies often satisfy the requirement of consent through "opt-out" policies that require the consumer to formally request that the company not share their information. Consumers may not even know the opt-out policy exists, or how to utilize it. Polls indicate that consumers strongly prefer an "opt-in" policy that requires they explicitly grant a company permission to collect and share their personal information (Equifax/Harris, 1996). It is clear that the principle of consent will require special consideration when deliberating any changes to U.S. privacy policy; otherwise it is highly likely that any new policy will experience the same difficulties Canada is experiencing

Chapter Summary

The data collected for this thesis clearly answers the primary question of this research. Canadian privacy policy is doing a more effective job of achieving the standard of the Fair Information Principles. Both the U.S. and Canadian governments have stated goals of achieving the consumer protections as outlined in the Fair Information Principles. The privacy policies of the two countries can be directly compared and possible improvements can be made to U.S. policy based on what has been learned from Canadian policy.

Based solely on the content analysis, PIPEDA appears to be a working model for change in the U.S., but the stakeholder analysis indicates that legislating a system like PIPEDA in the U.S. would face major challenges. The stakeholder analysis shows that both the law enforcement element of the U.S. government as well as much of American industry would be opposed to a legislated system like PIPEDA. The balancing act between individual rights, the marketplace, and law enforcement/security shown in the stakeholder analysis now become more evident in the content analysis. For example, PIPEDA has already been modified to permit national security exemptions. The following chapter will present several recommendations based on the results of both the content analysis and the stakeholder analysis.

Chapter 9: Conclusions and Policy Recommendations

This thesis has shown that current U.S. privacy legislation and regulations are not producing the level of consumer protection outlined by the FTC's Fair Information Principles. The FTC report released in 2000 concluded that the current body of legislation does not sufficiently implement the fair information practices and recommends additional legislation in conjunction with the current practice of industry self-regulation to achieve the desired fair information practices (FTC, 2000).

The 2005 EPIC report titled, "A Decade of Disappointment," found that industry self-regulation as a solution for privacy concerns has led to a situation in which consumers have lost virtually all of their bargaining power. Consumers do not have the right to control the information, or accuracy of that information, about them in the marketplace and as a result, companies are at a distinct advantage. There is little incentive for companies to provide privacy protection beyond the industry norm. The report characterizes the "exploitation of consumer transaction data as a classic example of market failure (EPIC, 2005)."

The 2006 Annenberg report concluded that consumer education initiatives were failing to achieve the desired level of consumer awareness. Consumers are confused regarding the meaning of a 'privacy policy' and interpret it to mean that its existence indicates a certain baseline level of protection provided by the company, which is incorrect. The Annenberg report also concluded that self-regulation is not worthwhile without a governing body, such as the FTC, setting benchmarks to measure progress. The Annenberg report concluded that unless the FTC can move beyond it's entirely

market based approach to privacy regulation, it will inevitably have to contend with additional legislation handed down by Congress (Turow, 2006).

Inadequacy of Existing Proposals

Chapter 2 highlighted several of the more recent comprehensive attempts at privacy legislation in the U.S. In reviewing each of the proposals as compared to the recommendations of the 1973 HEW report and the Fair Information Principles it is clear that none of the proposals address the problems with the currents system. The Consumer Privacy Protection Act of 2005 concentrated further on public education by mandating what kind of information must be provided to a consumer in a company's privacy policy. The proposal would do little more than legislate what is already the state of the industry in most cases. The proposal offers little in the way of additional protection.

The proposed Privacy Act of 2005 would provide consumers with the ability to block the sale or trade of their personal information, if they so chose. Unfortunately the proposed law is limited to those situations where the personal information is used by the purchasing organization for advertising or marketing purposes. The proposal attempts to address the Fair Information Principle of sharing, but it fails to do so adequately and does not address any of the other important Fair Information Principles. Both the FTC report (2000) and the Annenberg report (2006) demonstrated the ineffectiveness of piece-meal legislation that does more to confuse consumers than protect them.

Hillary Clinton's proposal titled, PROTECT Act of 2006, would also make it illegal for companies to allow personal data in their possession to be compromised through theft, loss, or data breach. The proposal does offer some avenues for those

victims of identity theft, but it fails to address several of the Fair Information Principles, such as the limitation of collection, and the limitation of use. The only protection offered to consumers by the PROTECT Act is the ability to exact compensation for damages from those companies that might be liable for their stolen identity or compromised personal information. The proposal is dramatic, but it fails to address the underlying problems.

Finally, the proposed Personal Data Privacy and Security Act of 2007 offered some severe penalties for companies whose data became compromised. It also would provide consumers with access to their information files maintained by data brokers (for a fee) and the ability to offer corrections to inaccuracies. However, the law did provide several exemptions and exceptions for data brokers that would allow them to avoid regulation in a way that weakens the policy. The rest of the Privacy and Security Act applied to government agencies and would do little to protect consumer's interactions with industry.

The review of current proposals made it clear that there is no pending U.S. legislation that would adequately address the problems facing consumers in the United States. The Canadian Parliament has taken steps aimed specifically at addressing the Fair Information Principles. This chapter will discuss results of the four research questions drawn from the two research analyses, and provide recommendations based on those findings.

Recommendations

The privacy policy analysis indicated a majority of the privacy policies available on U.S. websites only apply to transactions conducted through that website and do not apply to other consumer transactions with the company. This single result alone leaves a lingering question of, "what about the other types of transactions?" Are transactions that occur at the physical stores or offices devoid of any consumer information protections? When privacy policies are segmented and otherwise unavailable to would-be consumers, it becomes increasingly difficult for the consumer to be educated or make informed decisions about which companies they choose to give their business to.

Recommendation #1 – Any new privacy policy regarding how companies collect and manage personal information must mandate a baseline of protections based on the Fair Information Principles and provide for the enforcement of that mandate.

In comparison to those privacy policies available on Canadian websites, there was a stark difference. Companies that may have had vague or rather limited privacy policies available in the U.S., oftentimes had more consumer-friendly policies on their Canadian sites. Not only do more Canadian privacy policies apply to all consumer transactions, but the Canadian privacy policies themselves were more in line with the Fair Information Practices, as evidenced by the figures presented in Chapter 6. Canadian privacy policies received higher ratings in areas of Consent and Limitation of Use, which are two of the best indicators of adherence to the Fair Information Principles.

The stakeholder analysis conducted for this thesis found that while U.S. consumers are very much in favor of increased privacy protection and more rights over their personal information, there is strong resistance from some factions within government and industry. Law enforcement and national security agencies both in the United States and Canada resist privacy legislation because of the restrictions it may place on their ability to effectively gather information, locate criminals, and eliminate potential threats. In Canada, PIPEDA has already been amended to provide greater flexibility for national security agencies. In the U.S., law enforcement agencies work closely with private firms that are not restricted by the Privacy Act of 1974. These close partnerships with industry allow law enforcement and national security agencies to have access to extensive databases of information that they themselves are not allowed by law to collect.

Several industries, especially the data brokering and marketing industry in the United States are resistant to privacy legislation based on the Fair Information Practices as a dangerous "one size fits all" approach that does not consider the unique benefits of their industry. Representatives from these industries speak of the significant conveniences they provide to consumers that demand convenience. Similarly, industries in Canada are thriving under PIPDEA as identified in the NYMITY report which specifically highlights data broker Equifax as having one of the Top Privacy Policies in Canada (NYMITY, 2006).

Perhaps the most emotionally charged stakeholder is the individual consumer. The stakeholder analysis is full of examples of individual U.S. consumers that have become victims of either identity theft or incorrect records that they cannot access or

change. Victims have spent years trying to fight for non-existent rights in a system that has very little motivation to see their records corrected or their identity theft problems resolved. In Canada, consumers are still concerned about their privacy rights and their consent to the use of their information, but most have found PIPEDA to be a significant protection and the Office of the Privacy Commissioner has demonstrated an ability to arbitrate privacy problems in an efficient matter, oftentimes without the use of the court system.

The data examined in this research demonstrates that PIPEDA is providing more for consumer privacy in Canada than the multitude of U.S. privacy laws are doing for the privacy of U.S. consumers. The Canadian privacy policies studied in this research demonstrated a marked difference between those privacy policies posted to U.S. websites. The Canadian privacy policies were more aligned with the Fair Information Principles than the U.S. privacy policies from the same companies. There is a difference in effectiveness between the federal policies implemented in the U.S. and those in Canada and the Canadian, with policies achieving better results.

Recommendation #2 – The FTC should enforce the Fair Information Principles through regulation rather than legislation.

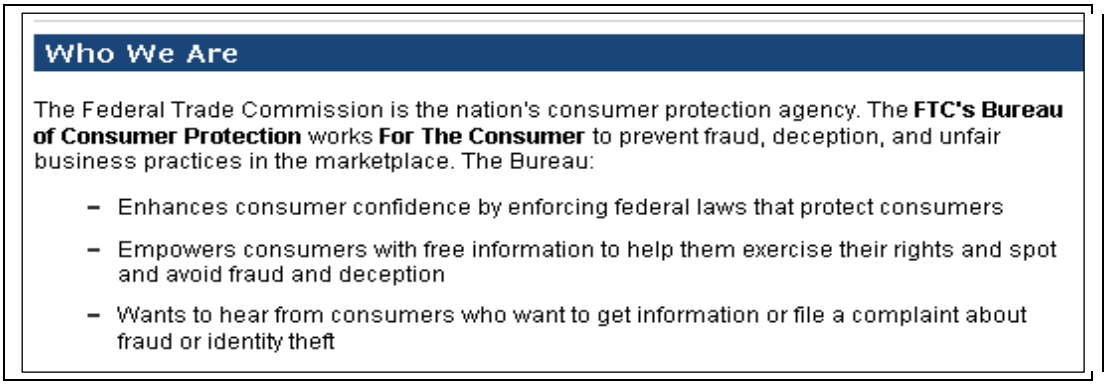
Rather than trying to copy Canada's legislation, it may be more effective to learn from Canada's experience. Canada's PIPEDA has made great strides toward improved privacy protection for consumers, but it has met with some significant challenges and has

already been amended to change parts of the law that were presenting problems for national security (Anti-Terror Act of 2001; Public Safety Act of 2002).

There is also evidence that Canadian companies, especially small businesses, are struggling with the principle of Consent outlined in PIPEDA. The principle of Consent also appears in the Fair Information Principles being pursued in the U.S. and requires that a company obtain a consumer's consent prior to collecting their information, prior to transferring that information to a third party, and prior to using the information for a purpose other than originally intended. This principle of Consent can require significant time and resources for a company that collects significant amounts of consumer data. In most cases, companies resolve this by offering an "opt-out" option that implies consent unless consent is specifically withdrawn by the consumer (CIPPIC, 2006).

Learning from Canada's experience with PIPEDA allows U.S. policymakers to craft a better solution for U.S. consumers, a solution that is more "tailor-made" to the needs of the U.S. market and companies in addition to the needs of U.S. consumers. Several of the problems with PIPEDA stem from the fact that PIPEDA is law and is required for all non-governmental entities that handle personal information. Studies from several different organizations in Canada have shown that many companies are struggling to catch up and attain compliance with the law (CIPPIC, 2006). The passage of PIPEDA and the creation of the Office of the Privacy Commission created substantial changes that forced industry to adapt to regulations or to fall behind and face harsh penalties. Instead, it may be wiser to work with an existing federal agency that already has a mandate to protect consumer privacy, such as the FTC. The FTC's website described their purpose as the consumer's protector (Figure 9A).

Figure 9A: The FTC's Bureau of Consumer Protection Mission Statement



Who We Are

The Federal Trade Commission is the nation's consumer protection agency. The **FTC's Bureau of Consumer Protection** works **For The Consumer** to prevent fraud, deception, and unfair business practices in the marketplace. The Bureau:

- Enhances consumer confidence by enforcing federal laws that protect consumers
- Empowers consumers with free information to help them exercise their rights and spot and avoid fraud and deception
- Wants to hear from consumers who want to get information or file a complaint about fraud or identity theft

The FTC has, within its authority, the ability to regulate matters of consumer protection. As part of that mandate, the FTC should pursue the issue of adherence to the Fair Information Principles as a rule rather than a suggestion. Currently, adherence to the Fair Information Principles is very loose and sometimes non-existent among companies in the U.S., as seen in the FTC's own reports and additional reports reviewed in Chapter 2. Companies routinely fail to obtain consent prior to the collection of personal information and in several cases share that information with third parties without offering their customers an opportunity to object.

In addition, regulation would provide greater flexibility than legislation. As conditions change the balance between individual rights, the marketplace, and security can be adjusted to meet the needs of all stakeholders. The FTC can continue to reevaluate stakeholder needs and adjust the regulations to accommodate.

Recommendation #3 – Companies should be given five years to make the necessary changes to comply with the Fair Information Principles

In order to be effective, the FTC would need to re-establish the Fair Information Principles much the way it is described on the agency's own website, as a code of conduct that has been well established and well defined out over the last quarter-century (FTC, 2000). The FTC would then mandate that, over the next half-decade, companies come into compliance with the Principles. In order to be considers in-compliance; a company must demonstrate its adherence to the principles in all interactions with consumer personal data, not just those that occur through their website(s). The Fair Information Principles are provided in Appendix D as they are listed on the FTC website.

Recommendation #4 – Early adopters of the Fair Information Principles should receive a certificate of compliance that will give them the competitive advantage of providing protections their competition is not able to duplicate.

Organizations able to prove their adherence to the Fair Information Principles in less than the allotted time would receive a certificate of compliance that would give them a competitive advantage in their industry prior to the time when compliance becomes mandatory. Since U.S. industry is far from compliance with the Fair Information Principles, there must be a significant adjustment period permitted. Canada provided their industries with a period of two years in which to achieve compliance. It is clear that while Canadian industry is already well ahead of their American counterparts in terms of compliance with the Fair Information Principles, they have not achieved the desired level

of protection and many small businesses are in the position of being out of compliance with a law that can have expensive financial consequences.

Recommendation #5 – FTC imposed fines and lawsuits raised by consumers should be the enforcement mechanism, when companies fail to meet FTC regulations.

Expensive financial penalties should be used as an enforcement mechanism only after the end of the decade-long implementation, and only against companies that fail to meet their obligations to consumers. Companies that fail to meet the requirements of the Fair Information Principles regulated by the FTC must be fined severely enough, as to encourage compliance. Also, consumers must be able to file complaints with the FTC against companies that are believed to be in violation of the Fair Information Principles mandated by the agency.

Advantages of Recommendations

There are two major advantages to implementing the outlined recommendations rather than Congress attempting to pass major legislation to enforce the Fair Information Principles.

Consumer Choice

The goal of an FTC certification program would be to provide consumers with a fundamental baseline of protection on which to base their decisions. The reports and

studies reviewed in Chapter 2 indicated that current consumer education programs are failing to inform consumers of their rights, and of the options available to them. This failure to inform consumers is not due a lack of information, but more likely due to information that is complex, confusing, and overwhelming at the same time. There are no well established standards for industry privacy policies and customers often find themselves trying to read-between-the-lines of legal jargon and vague claims of protection. By providing a full half-decade in which consumers can become acclimated with rights afforded them by the Fair Information Principles and a full decade for companies to ensure they can implement compliant systems and training, an FTC regulatory system can be more effective and more flexible for both consumers and industry.

Industry Flexibility

PIPEDA was signed into law in April of 2000, but the law did not apply to all companies until January 1, 2004. PIPEDA provided industry with over three and a half years to prepare for the law, but during that time consumers did not know which businesses had already achieved compliance. Testimony reviewed in Chapter 7 demonstrated that industry is hesitant to accept greater restrictions over their business activities for privacy concerns. Those who testified raised issues about customer convenience and cost of service. The concern is that customers are accustomed to fast and convenient service and increased regulation could potentially slow service and impede transaction speed. Increased regulation, it was argued, could also drive up costs

for consumers. The chief privacy officer for DoubleClick argued that much of Internet content is free because of the ability for companies to use advertising income to cover costs (Wunsch, 2006; Faley, 1999; Polonetsky, 2000).

The concerns raised by industry representatives over the possible effects of increased regulation of personal information could be studied over the suggested time period. Over the course of the grace period, some companies would implement the new rules faster than others. Some companies would be able to achieve the FTC certificate early on in the decade and would be able to report the repercussions, if any, while implementing the Fair Information Principles. The recommended half-decade of transition would provide the FTC much more information on which to base future implementation of privacy regulations. Since PIPEDA is still quite young in Canada, there is little published information regarding the effects the law has had on customer costs and convenience. An additional five years will provide a wealth of information from the Canadian market, as well as the ability to study the early effects of increased regulation on the U.S. market.

Chapter Summary

This chapter outlined a summary of the research findings and concluded that the current course of action chosen by the FTC, and the U.S. government is not providing an effective solution to consumers' privacy concerns. The reports from the FTC, EPIC, and Annenberg school all showed deficiencies in the current regulatory system that were resulting in confusion on the part of consumers and inadequate response on the part of industry.

It was also demonstrated that current proposals before Congress for additional legislation are also inadequate to the task of effective change either because they fail to address the breadth of the problem or they do not step outside the current failing framework of industry self regulation and consumer education.

Finally, this thesis has demonstrated that Canada's PIPEDA legislation has achieved a significant level of success at moving Canadian industry closer to compliance with the Fair Information Principles that is also the stated goal of the U.S. FTC (FTC, 1996). While not wholly successful, PIPEDA has shown results much better than those achieved under the current U.S. regulatory body.

It was then concluded that the U.S. needs to implement a new course of action and it is appropriate to review PIPEDA for successful approaches. Rather than pursuing a piece of sweeping legislation like PIPEDA, that creates another government agency and a new body of laws, it is preferable for an existing agency like the FTC to institute a modified regulation through an existing agency framework. The regulation change should be to mandate compliance with the well-established Fair Information Principles that were developed in 1973 by the U.S. government and which are also the basis for Canada's PIPEDA.

Chapter 10: Limitations and Future Work

This thesis was conducted based on the assumption that U.S. consumers are unsatisfied with the current level of privacy policy in their country. There is frequent media coverage of identity theft, data theft, profiling, wiretapping, and surveillance. The literature review conducted for this thesis provided a history of privacy advocacy in the United States and a strongly held tradition of individualism and personal privacy. It is with that assumption that this thesis was developed and conducted.

One of the first reports collected for the literature review was the 2006 Privacy International Survey that indicates the United States as one of the lowest-scoring developed countries in their survey of privacy protections (Privacy International, 2007). At the same time, Canada received some of the best scores in the survey. With Canada being such a close neighbor and trading partner, it was the natural choice for comparison.

Two different research methodologies were combined to answer the questions posed for this thesis. The content analysis and the stakeholder analysis provided different results, which when combined, provides answers to both the results different national policies are achieving and why those policies are achieving the results they are experiencing. There are limitations associated with the methodology and data sources included in this research, which must be acknowledged. This thesis does not answer all possible questions that could be posed regarding this topic. There are opportunities for additional research in the field of U.S. privacy policy.

The thesis was limited to a one-year time frame with one researcher working part time. The goals of the project were completed and the expected results realized. However, further study could have been achieved with additional time and resources.

Content Analysis

The first method used content analysis to compare company privacy policies against the standards of the Fair Information Principles. While the content analysis provided rather useful data, it was conducted on only 43 company privacy policies. A greater number of policies would have provided additional data on other industries and on companies. Examining additional industries would provide more in-depth context to the comparison. It is probable that companies in the healthcare and airline industries, along with others, may have unique perspectives on privacy policy and consumer's personal information. Due to the personnel and time constraints, it was prohibitive to analyze additional companies or industries.

The data was gathered from those privacy policies that had been posted to company websites and was freely available to the public. In cases where the website privacy policy was limited in scope to only online activity, the content analysis was unable to account for business transactions that occur outside of the company website. There were also a limited number of industries and companies sampled for the data set. Additional industries and companies may provide richer results, but the additional time necessary was not possible for this project. The content analysis was conducted by a sole researcher with all judgments and categorization relying on a single opinion. The content analysis could have been conducted based on the judgments of multiple researchers or even in a random survey of the public to obtain a different assessment of how each company privacy policy measured up to the Fair Information Principles.

Stakeholder Analysis

The stakeholder analysis is based entirely on materials obtained freely over the internet, including articles, press releases, congressional testimony and published reports. Additional information could have been gathered through interviews or surveys of stakeholders and their positions. The stakeholder positions provided in this research are summations compiled by a single researcher. Bias could have been reduced through a diverse team of researchers. These other methods could have provided additional information, but would have consumed substantially more time and resources to execute.

The stakeholder analysis is intended to provide the prospective and positions of three major stakeholder groups. Materials that are freely available on the Internet must be verified for authenticity. This was done by only using material from U.S. and Canadian government agency websites, industry trade group websites, and consumer advocacy sites that are well established in the privacy community. There are still limitations to this type of information gathering. Data that is collected from secondary sources could be misinterpreted or used outside the proper context. Interviews and direct interaction with agency or organizational representatives could reduce the risk of misinterpretation or misunderstanding.

Future Work

This thesis lays the ground work for additional research into the topic of U.S. federal privacy policy. The results of this research provided answers to the four research questions outlined in Chapter 4, but these are only partial answers. Based on the results, it appears that Canadian privacy policy (PIPEDA) is achieving results that more closely

align with the Fair Information Principles. However, it is unclear whether those results are due only to the enforcement mechanisms outlined in PIPEDA. Additional research could be done to examine other possible reasons for the varying results. It also seems clear that different industries are impacted differently by changes to federal privacy policy. PIPEDA is only one of an infinite number of solutions that could be used to correct perceived deficiencies in U.S. privacy policy. Additional research could provide a more complete understanding of the effects specific changes could have on industries. This information would assist in crafting a more tailored policy that would have the maximum benefit, while possibly reducing the number of problems encountered.

Future research initiatives in this topic area would need to focus on discovering the specific motivations of various stakeholders and discovering additional causes for the failure to achieve the Fair Information Principles in the U.S. and the better results being achieved by Canada. To achieve these goals, future research initiatives are recommended in Figure 10A.

Figure 10A: Summary of Future Research Opportunities

- Interviews with representatives of the FTC, Trade Organizations, and Consumer Advocacy organizations.
- Survey of company privacy officers for their viewpoint
- In-depth analysis of legislative efforts and lobbying activities.

Chapter Summary

This thesis demonstrates a clear need for change in U.S. privacy policy. The FTC and consumers are unsatisfied with the protections afforded by current policy. Conversely, companies have very real concerns regarding possible changes that have

been recommended by legislators and groups such as EPIC and CDT. The Canadian policy of legislation, such as PIPEDA, appears to be working for Canada, but attempts at enforceable legislation in the U.S. have been unsuccessful to date. This thesis provides a partial picture of the current situation and offers recommendations for positive change and future research that could provide additional information. Continued research is important to achieving the best privacy policy for all stakeholders involved. The policy lifecycle includes continuing assessment of policy results and implementation of adaptive changes.

Appendix A: Acronyms

CDT – Center for Democracy and Technology

CIPPIC - Canadian Internet Policy and Public Interest Clinic

CMA - Canadian Marketing Association

EPIC - Electronic Privacy and Information Center

EPPA - Employee Polygraph Protection Act

FTC – Federal Trade Commissioner

GAO - Government Accountability Office

HEW - Health Education and Welfare (Department of, Secretary of)

HIPAA - Health Insurance Portability and Accountability Act

OMB - Office of Management and Budget

PI – Privacy International

PIPEDA - Personal Information Protection and Electronic Documents Act

PPRS – Privacy Policy Rating System

PROTECT - Privacy Rights and Oversight for Electronic and Commercial Transactions

SIN - Social Insurance Number

Appendix B: U.S. Companies Examined

CitiFinancial - http://www.citifinancial.com

HSBC - http://www.hsbcusa.com

Chase - http://www.chase.com

JP Morgan - http://www.jpmorgan.com

Wachovia - http://www.wachovia.com

Wells Fargo - https://www.wellsfargo.com

Accenture - http://www.accenture.com

Axiom - http://www.acxiom.com

ChoicePoint - http://www.choicepoint.com

LexisNexis - http://www.lexisnexis.com

SRA International - http://www.sra.com

DST Systems - http://www.dstsystems.com

Equifax – http://www.equifax.com

First Data - http://www.firstdata.com

Fiserv - http://www.fiserv.com

GMAC - http://www.gmacfs.com

Mastercard - http://www.mastercard.com

Sungard - http://www.sungard.com

Allstate - http://www.allstate.com

Statefarm - http://www.statefarm.com

Amazon – http://www.amazon.com

Costco - http://www.costco.com

Ticketmaster – http://www.ticketmaster.com

Ebay – http://www.ebay.com

Wal-mart – http://www.walmart.com

ACNielson - http://www2.acnielsen.com

DoubleClick - http://www.doubleclick.com

Market Research - http://www.marketresearch.com

Vertis - http://www.vertisinc.com

AOL – http://www.aol.com

Expedia – http://www.expedia.com

Travelocity – http://www.travelocity.com

Burger King – http://www.burgerking.com

McDonald's – http://www.mcdonalds.com

Taco Bell – http://www.tacobell.com

FedEx – http://www.fedex.com

UPS – http://www.ups.com

AT&T - http://www.att.com

Bell South - http://www.bellsouth.com

Comcast - http://www.comcast.com

Sprint/Nextel - http://www.sprint.com

Verizon - http://www.verizonwireless.com

Appendix C: Canadian Companies Examined

CitiFinancial - http://www.citifinancial.ca

HSBC - http://www.hsbc.ca

Wells Fargo - http://financial.wellsfargo.com

LexisNexis - http://www.lexisnexis.ca

Equifax – http://www.equifax.com/EFX_Canada/

GMAC - http://www.gmcanada.com

Mastercard - http://www.mastercard.com/ca

Allstate - http://www.allstate.ca/

Statefarm - http://www.statefarm.ca

Amazon – http://www.amazon.ca

Costco - http://www.costco.ca

Ticketmaster – http://www.ticketmaster.ca

Ebay – http://www.ebay.ca

Wal-mart – http://www.walmart.ca

DoubleClick - http://www.doubleclick.com/us/about_doubleclick/privacy/canada.asp

AOL - http://canada.aol.com

Expedia - http://www.expedia.ca

Travelocity - http://www.travelocity.ca

Burger King – http://www.burgerking.ca

McDonald's – http://www.mcdonalds.ca

Taco Bell – http://www.tacobell.ca

FedEx - http://www.fedex.com/ca_english/privacycode.htm

UPS - http://www.ups.com/content/ca/en/privacy.html

AT&T – http://www.att.ca

Spint/Nextel – http://www.spint.com

Appendix D: Fair Information Principles (FIPS) on FTC.gov

http://www.ftc.gov/reports/privacy3/fairinfo.shtm

A. Fair Information Practice Principles Generally

Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information -- their "information practices" -- and the safeguards required to assure those practices are fair and provide adequate privacy protection.(27) The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices.(28) Common to all of these documents [hereinafter referred to as "fair information practice codes"] are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

1. Notice/Awareness

The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.(29) Moreover, three of the other principles discussed below -- choice/consent, access/participation, and enforcement/redress -- are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.(30)

While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:

- identification of the entity collecting the data;(31)
- identification of the uses to which the data will be put;(32)
- identification of any potential recipients of the data;(33)
- the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);(34)
- whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information;(35) and
- the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.(36)

Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the data;(37) whether the consumer has been given a right of access to the data;(38) the ability of the consumer to contest inaccuracies;(39) the availability of redress for violations of the practice code;(40) and how such rights can be exercised.(41)

In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any Web page where information is collected from the consumer. It

should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.

2. Choice/Consent

The second widely-accepted core principle of fair information practice is consumer choice or consent.(42) At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information -- *i.e.*, uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer.(43) Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put.(44) Thus, for example, consumers can be provided separate choices as to whether they wish to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a website, thus effectively eliminating any need for default rules.(45)

3. Access/Participation

Access is the third core principle. It refers to an individual's ability both to access data about him or herself -- *i.e.*, to view the data in an entity's files -- and to contest that data's accuracy and completeness.(46) Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.(47)

4. Integrity/Security

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.(48)

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.(49) Managerial measures include internal organizational measures that limit access to data and ensure that those

individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.(50)

5. Enforcement/Redress

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.(51) Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.(52)

a. Self-Regulation(53)

To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress).(54) Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association;(55) external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue.(56) A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.(57)

Appropriate means of individual redress include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed.(58) Thus, a self-regulatory system should provide a means to investigate complaints from individual consumers and ensure that consumers are aware of how to access such a system.(59)

If the self-regulatory code has been breached, consumers should have a remedy for the violation. Such a remedy can include both the righting of the wrong (*e.g.*, correction of any misinformation, cessation of unfair practices) and compensation for any harm suffered by the consumer.(60) Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation.

b. Private Remedies

A statutory scheme could create private rights of action for consumers harmed by an entity's unfair information practices. Several of the major information practice codes, including the seminal 1973 HEW Report, call for implementing legislation.(61) The creation of private remedies would help create strong incentives for entities to adopt and implement fair information practices and ensure compensation for individuals harmed by misuse of their personal information. Important questions would need to be addressed in such legislation, *e.g.*, the definition of unfair information practices; the availability of compensatory, liquidated and/or punitive damages;(62) and the elements of any such cause of action.

c. Government Enforcement

Finally, government enforcement of fair information practices, by means of civil or criminal penalties, is a third means of enforcement. Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers.(63) Whether enforcement is civil or criminal likely will depend on the nature of the data at issue and the violation committed.(64)

Bibliography

Accenture. Accenture Privacy Policy. 1996. 18 Feb. 2007 <http://www.accenture.com>. Privacy Policy for Accenture.com. Most U.S. Data Brokers, including Accenture, had privacy policies that were limited in scope to those transactions that occurred between customers and the company website. No other transactions were covered.

ACNielson. ACNielsen.com - Privacy Policy. 18 Feb. 2008 <http://www2.acnielsen.com>. Privacy Policy for ACNielson. There wasn't a separate policy for Canada.

Acxiom. Online Privacy Policy. 21 Dec. 2004. 18 Feb. 2007 <http://www.acxiom.com>. Acxiom's online privacy policy. As with other Data Brokers, Acxiom's privacy policy only applied to those transactions that occur between the customer and the Acxiom website.

Alderman, Ellen, and Caroline Kennedy. The Right to Privacy. N.p.: Vintage, 1997.

Allstate. Allstate Canada Privacy Brochure. 17 Feb. 2007 <http://www.allstate.ca>. Allstate Canada privacy policy brochure. Allstate is categorized as a member of the Insurance group of companies.

- - -. Allstate Privacy Statement. 26 Oct. 2006. 16 May 2007 <http://www.allstate.com>. Allstate's U.S. privacy policy. Allstate is categorized as a member of the Insurance group of companies.

Amazon.ca. Amazon.ca Privacy Notice. 21 Apr. 2006. 18 Feb. 2007 <http://www.amazon.ca>. Privacy policy for Amazon in Canada.

Amazon.com. Amazon.com Privacy Notice. 27 Oct. 2005. 18 Feb. 2007 <http://www.amazon.com>. Privacy policy for Amazon.com in the U.S.

Anthony, Sheila F. "Online Privacy Protection Testimony of FTC Commissioner." U.S. Senate Committee on Commerce, Science, and Transportation. 25 May 2000. 15 Feb. 2007 <http://commerce.senate.gov>.

Ant-Terror Act . Winter 2001. A law rushed through parliament just after the events of September 11th 2001. Some parts of the law were later found to be unconstitutional by the Canadian court system.

AOL Canada. AOL.ca - Privacy Policy. 2006. 13 Apr. 2007 <http://canada.aol.com/>. Privacy Policy for AOL Canada.

AOL US. AOL Network Privacy Policy. 3 Apr. 2006. 13 May 2007 <http://www.aol.com>. Privacy Policy for AOL U.S.

AT&T. AT&T Privacy Notice. 16 June 2006. 17 Feb. 2007 <http://www.att.com/privacy/policy/#3>. Privacy Policy for AT&T Canada.

- - -. AT&T Privacy Notice. 16 June 2006. 17 Feb. 2007 <http://www.att.com/privacy/policy/#3>. Privacy Policy for AT&T.

Ball, Tom. "Privacy Measures Being Overlooked." Editorial. London Free Press [Ontario] 28 Feb. 2005, Final Edition ed.: A8. LexisNexis Academic. LexisNexis. 29 Oct. 2006 <http://web.lexis-nexis.com/universe>.

Beres, Ed. "Information freeze." Editorial. Peterborough Examiner [Ontario] 30 May 2005, Final Edition ed., sec. OPINION: Pg. A4. The author complains that the officials that are supposed to be providing information under PIPEDA know

nothing of the law and as a result are providing very little information. The author remains critical of officials and supportive of the privacy laws.

Biden, Joeseph R. "No President Is Above Our Constitution." US Fed News 1 Jan. 2006. LexisNexis Academic. LexisNexis. 22 Oct. 2006 <http://web.lexis-nexis.com/universe>.

Bouckaert, Jan, and Hans Degryse. "Opt In Versus Opt Out: A Free-Entry Analysis of Privacy Policies." Paper presented at The Fifth Workshop on the Economics of Information Security (WEIS 2006) . 30 Jan. 2008 <http://weis2006.econinfosec.org/prog.html>.

Boxer, Barbara. Identity Theft. US Senate Committee on Commerce, Science, & Transportation. 16 June 2005. 18 Feb. 2007 <http://commerce.senate.gov>.

BREMNER, Adam. "Transactional Customers Form A Growing High-Margin Niche." American Banker 27 Oct. 2000: 13. ABI/INFORM. ProQuest. 1 Apr. 2007 <http://proquest.umi.com/login>.

Brown v. Texas. No. 77-6673. Supreme Court of the United States. 25 June 1979 <http://www.law.cornell.edu>. The application of the Texas statute to detain appellant and require him to identify
himself violated the Fourth Amendment because the officers lacked any reasonable suspicion to believe that appellant was engaged or had engaged in criminal conduct.

Brugha, Ruairi. "Stakeholder Analysis: A Review." Health Policy and Planning (2000): 239-246.

Burger King. BurgerKing.com General Online Privacy Policy. 1 Apr. 2005. 16 May 2007 <http://www.burgerking.com>. Privacy Policy for BurgerKing U.S.

Burger King Canada. Burger King - Privacy Policy. 2005. 13 May 2007 <http://www.burgerking.ca>. Privacy Policy for Burger King Canada.

The Canadian Internet Policy and Public Interest Clinic (CIPPIC). Compliance with Canadian Data Protection Laws: Are retailers measuring up? . 2006. 7 July 2007 <idtrail.org/index2.php?option=com_content&do_pdf=1&id=442>.

- - -. On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship. 2006. 7 July 2007 <http://www.cippic.ca>.

Canadian Press. "Privacy commissioner not convinced police need new spying rules." The Record [Kitchener-Waterloo] 1 Sept. 2006, Final Edition ed.: D11.

Canadian Standards Association. Model Code for the Protection of Personal Information. N.p.: n.p., 1996. A set of ten principals later adopted by the Privacy Commissioner of Canada that dictate how organizations should handle the personal data of individuals.

Canadian Standards Association (CSA). "CSA - Standards - About the Privacy Code - Privacy Code." CSA Website. 2008. 3 Mar. 2008 <http://www.csa.ca/standards/privacy/code/Default.asp?language=english>. This is the first edition of CSA Model Code for the Protection of Personal Information.

Center for Democracy and Technology (CDT). Following the Money: How Advertising Dollars Encourage Nuisance and Harmful Adware and What Can be Done to Reverse the Trend. 2006. 20 Feb. 2007 <www.cdt.org/privacy/20060320adware.pdf>.

- - -. Following the Money II: The Role of Intermediaries in Adware Advertising. 2006. 20 Feb. 2007 <www.cdt.org/privacy/20060809adware.pdf>.

Cerasale, Jerry, and Ronald Plesser. "Comments of The Direct Marketing Association." Federal Trade Commission. 30 Nov. 1999. 2 May 2007 <http://www.fte.gov>.

Chase Bank. Privacy Policy. 1 Sept. 2006. 17 Feb. 2007 <http://www.chase.com>. Privacy Policy for Chase Bank. No separate policy was provided for interactions with Canadian customers.

Children's Online Privacy Protection Act of 1998. Pub. L. 105-277. 21 Oct. 1998. 9 Jan. 2008 <http://www.ftc.gov>. The act, effective April 21, 2000, applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing to those under 13.

ChoicePoint. ChoicePoint - Privacy Policy. 19 June 2006. 18 Feb. 2007 <http://www.choicepoint.com>. ChoicePoint's online privacy policy. As with other Data Brokers, ChoicePoint's privacy policy only applied to those transactions that occur between the customer and the ChoicePoint website.

- - -. Privacy at ChoicePoint: Advocacy. 18 Feb. 2007 <http://www.privacyatchoicepoint.com/advocacy/index.html>.

"ChoicePoint: More ID theft warnings: ID company says criminals able to obtain almost 140,000 names, addresses and other information." CNN.com 17 Feb. 2005. 29 Oct. 2006 <http://www.cnn.com>.

CitiFinancial. "Privacy Policy." Citigroup Privacy Promise for Consumers. 1 July 2006. 17 Feb. 2007 <http://www.citifinancial.com/common/citigroup_privacy.php>. Privacy Policy available through CitiFinancial's U.S. website. Used for company privacy policy analysis.

Citigroup Canada. Privacy of Personal Information Statement. 1 Sept. 2006. 17 Feb. 2007 <http://www.citi.com/citigroup/global/can.htm>. Citigroup Canada's privacy policy. A 20-page PDF document available for download on the company's website. The document details what information the company collects and how it is used.

Clinton, Hillary. Remarks of Senator Hillary Rodham Clinton on Privacy. American Constitution Society. 16 June 2006. 25 Sept. 2006 <http://clinton.senate.gov>.

- - -. Senator Clinton Opens 2006 National Convention with Major Policy Address on Privacy. 2006. American Constitution Society. American Constitution Society. 18 Oct. 2007 <http://www.acslaw.org/node/2967>. On June 16, Senator Hillary Rodham Clinton (D-NY) delivered the opening address of the ACS 2006 National Convention with a major policy address on privacy in which she announced new proposed legislation to address the security of private information. Declaring privacy to be "synonymous with liberty," Senator Clinton called for greater

federal protection for personal data from theft or misuse by private commercial actors, as well as greater Congressional and judicial oversight over domestic surveillance and data-mining programs unilaterally crafted by the executive branch.

Cloud, Morgan. "The Bugs in Our System." The New York Times 13 Jan. 2006. LexisNexis Academic. LexisNexis. 22 Oct. 2006 <http://web.lexis-nexis.com/universe>.

Cockfield, Arthur J. The State of Privacy Laws and Privacy- Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government. 2004. 2 Oct. 2006 <http://www.uoltj.ca/articles/vol1.1-2/2003-2004.1.1-2.uoltj.Cockfield.325-344.pdf>.

Consumer Privacy Protection Act of 2005. Pub. L. H. R. 1263. 10 Mar. 2005. 24 Sept. 2006 <http://thomas.loc.gov>. A Bill to protect and enhance consumer privacy.

Costco Wholesale Canada. Costco Wholesale Canada Ltd Customer Privacy Statement. 15 Oct. 2004. 15 Oct. 2006 <http://www.costco.ca>. Privacy Statement for Costco Canada.

Costco Wholesale Corporation. Costco Wholesale Corporation Privacy Statement. May 2004. 15 Oct. 2006 <http://ww.costco.com>. Privacy Statement for Costco U.S.

CP. "Privacy Commissioner Questions Federal Plans for Internet Surveillance." Fort McMurray Today [Ottawa] 1 Sept. 2006, Final Edition ed.: A4. LexisNexis Academic. LexisNexis. 29 Oct. 2006 <http://web.lexis-nexis.com/universe>.

Curling, Douglas C. “Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use.” U.S. Senate Committee on the Judiciary. 13 Apr. 2005. 18 Feb. 2007 <http://judiciary.senate.gov>.

David, Elder. “Changes to Bell Sympatico Service Agreement .” Interview with Terry McQuay. NYMITY Inc. Aug. 2006. 5 Nov. 2006 <http://www.nymity.com/privaviews/2006/elder2.asp>. David Elder, the Assistant General Counsel for Bell Canada, Canada’s leading communications company, outlined his top ten lessons learned from 3 years of operating under PIPEDA.

DeBare, Ilana. “All businesses are subject to laws protecting customers’ privacy.” The San Francisco Chronicle 11 Jan. 2006, FINAL Edition ed.: C1. LexisNexis Academic. LexisNexis. 1 Apr. 2007 <http://web.lexis-nexis.com/universe>.

Dempsey, James. “Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use.” Senate Committee on the Judiciary. 13 Apr. 2005. 18 Feb. 2007 <http://judiciary.senate.gov/print_testimony.cfm?id=1437&wit_id=2875>.

Dempsey, James X, and Lara M Flint. Commercial Data and National Security. Center for Democracy and Technology (CDT), 2004. 17 Dec. 2007 <www.cdt.org/publications/200408dempseyflint.pdf >.

DoubleClick. Privacy - DoubleClick Inc. 17 Feb. 2007 <http://www.doubleclick.com>. Privacy policy for DoubleClick USA.

DoubleClick Canada. Canada - DoubleClick Inc. 18 Feb. 2007 <http://www.doubleclick.com/us/about_doubleclick/privacy/canada.asp>. Privacy policy for DoubleClick Canada.

DST Systems, Inc. Privacy Policy. 17 Feb. 2007 <http://www.dstsystems.com>. The online privacy policy for DST Systems Inc. DST is categorized as a member of the Financial Data Services group.

Ebay. Ebay Privacy Policy. 8 Oct. 2006 <http://www.ebay.com>. Privacy Policy for Ebay in the U.S.

Ebay Canada. Ebay Privacy Policy. 8 Oct. 2006 <http://www.ebay.ca>. Privacy Policy for Ebay Canada.

Elder, David. "Changes to Bell Sympatico Service Agreement." Interview with Terry McQuay. NYMITY.ca. Aug. 2006. 5 Nov. 2006 <http://www.nymity.com/privaviews/2006/elder2.asp>.

Electronic Privacy Information Center. "Public Opinion on Privacy." EPIC.com. 27 Apr. 2007. 5 Mar. 2008 <http://epic.org/privacy/survey/>.

- - -. "Total 'Terrorism' Information Awareness (TIA)." EPIC.com. 21 Mar. 2005. 14 Aug. 2007 <http://www.epic.org/privacy/profiling/tia>.

- - -. "The USA PATRIOT Act." EPIC.com. 17 Nov. 200 <http://www.epic.org/privacy/terrorism/usapatriot/>.

Electronic Privacy Information Center (EPIC). 13 Nov. 2006 <http://www.epic.org>.

Electronic Privacy Information Center (EPIC). "Public Opinion on Privacy." EPIC Public Opinion and Privacy Page. 27 Apr. 2007. 3 June 2007 <http://www.epic.org/privacy/survey/>.

Electronic Privacy Information Center (EPIC), and Chris Jay Hoofnagle. Privacy Self Regulation: A Decade of Disappointment . 2005. 29 Mar. 2007 <http://www.epic.org>.

Eltis, Karen. “THE Emerging American Approach To E-Mail Privacy In The Workplace: Its Influence On Developing Case Law In Canada And Israel: Should Others Follow Suit? .” University of Illinois, College of Law. 12 Oct. 2004. 5 Feb. 2007 <http://www.law.uiuc.edu/publications/CLL&PJ/archive/vol_24/issue_3/EltisArticle24-3.pdf>.

Equifax. Equifax Canada’s Commitment to Privacy. 24 Mar. 2006. 8 Oct. 2006 <http://www.equifax.com/home/en_ca>. The privacy policy of Equifax Canada. Equifax is classified as a member of the Financial Data Services group of companies.

- - -. Equifax Online Privacy Policy & Fair Information Principles. 5 Oct. 2006. 8 Oct. 2006 <http://www.equifax.com>. The privacy policy of Equifax in the U.S. Equifax is categorized as a member of the Financial Data Services group of companies.

Equifax, and Harris. 1996 Equifax/Harris Consumer Privacy Survey. 30 Jan. 2008 <http://www.mindspring.com>.

Expedia. Expedia.ca Expedia.ca’s Privacy Pledge. 13 Apr. 2007 <http://www.expedia.ca>. Privacy Policy for Expedia Canada.

- - -. Expedia.com Privacy Policy. 1 Dec. 2006. 13 May 2007 <http://www.expedia.com>. Privacy Policy for Expedia US.

The Federal Trade Commission. FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers. 3 Sept. 2003 <http://www.ftc.gov/opa/2003/09/idtheft.shtm>.

Federal Trade Commission (FTC). Anticipating the 21 Century: st Consumer Protection Policy in the New High-Tech, Global Marketplace. 1996. 2 May 2007 <www.ftc.gov/opp/global/report/gc_v2.pdf>.

Federal Trade Commission (FTC). Nation's Big Three Consumer Reporting Agencies Agree To Pay $2.5 Million To Settle FTC Charges of Violating Fair Credit Reporting Act. 13 Jan. 2000. 13 Aug. 2000 <http://www.ftc.gov>.

Federal Trade Commission (FTC). Privacy Online: Fair Information Practices in the Electronic Marketplace. 2000. 25 Apr. 2007 <www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

Federal Trade Commission (FTC). Protecting Personal Information Federal Trade Commission: A Guide for Business. 16 Apr. 2007 <www.ftc.gov/infosecurity/>.

Federal Trade Commission (FTC). Read Up! How to be an Informed Consumer . 3 May 2007 <www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf>.

FedEx. Federal Express Canada Ltd. Privacy Code. 13 May 2007 <http://www.fedex.com/ca_english/privacycode.html>. Privacy Policy for FedEx Canada.

- - -. Privacy Policy for "fedex.com." 2007. 13 May 2007 <http://www.fedex.com/us/privacypolicy.htm>. Privacy Policy for FedEx U.S.

"Filene's Bans Sisters for Complaints." RedOrbit.com 13 July 2003. 1 Apr. 2007 <http://www.redorbit.com>.

Findlay, Alan. “Canucks’ info at risk; U.S. could subpeona our records under their laws.” The Toronto Sun [Ottawa] 16 Apr. 2007, FINAL EDITION ed.: 7. LexisNexis Academic. LexisNexis. 6 June 2007 <http://web.lexis-nexis.com/universe>.

First Data. First Data - Privacy. 28 Sept. 2006. 17 Feb. 2007 <http://www.firstdata.com>. The privacy policy for First Data U.S. First Data is categorized as a member of the Financial Data Services group of companies.

Fiserv. Fiserv - Privacy Policy. 2006. 17 Feb. 2007 <http://fiserv.com>. The privacy policy for Fiserv. Fiserv is categorized as a member of the Financial Data Services group of companies.

“Fortune 500 2006.” CNN. 2007. 17 Feb. 2007 <http://www.money.cnn.com>.

Frank, Mari. “Hearing on Identity Theft/Data Broker Services.” United States Senate Committee On Commerce, Science And Transportation. 10 May 2005. 18 Feb. 2007 <http://commerce.senate.gov>.

Freed, Joshua. “The customer is always right? Not anymore .” Deseret News [Minneapolis] 5 July 2004. 6 Dec. 2008 <http://www.deseretnews.com>.

Geist, Michael. “Top court tips its hand on privacy: Canada’s privacy commissioner needs more clout, supreme court says.” Ottawa Citizen 11 May 2006: Pg. E5. The Supreme Court of Canada sites several reasons why the Office of the Privacy Commissioner of Canada did not have sufficient power to fulfill the role of the office and says the office should be empowered to fulfill its role properly.

George, Orwell. 1984. London: Secker and Warburg, 1949. The book that first introduced the all-knowing government of “Big Brother” and the surveillance

society in which the books characters were controlled completely by the omnipresent government.

GMAC. GMAC Privacy US. 2007. 13 May 2007 <http://www.gmacfs.com>. GMAC Financial Services privacy policy. GMACFS is categorized as a member of the Financial Data Services group of companies.

GMAC Canada. GMAC Privacy Canada. 13 May 2007 <http://www.gmcanada.com>. GMAC Canada privacy policy. GMAC is categorized as a member of the Financial Data Services group of companies.

Gordon, Marcy. "Some Banks Make Hard Time For Clients Who Want Privacy Customers Find Bulky System For Protecting Personal Data." St. Louis Post - Dispatch 31 Aug. 2001: B1.

Graves, Lisa. "Openness in Government and Freedom of Information: Examining the OPEN Government Act of 2005." United States Senate Committee on the Judiciary. 15 Mar. 2005. 18 Feb. 2007 <http://judiciary.senate.gov>.

Greenemeier, Larry. "Data Grab; The feds want data for security and crime fighting, and businesses have what they need. The trick is knowing what to share and where to draw the line." INFORMATIONWEEK (June 2006): 23. LexisNexis Academic. LexisNexis. 1 Apr. 2007 <http://web.lexis-nexis.com/universe>.

Griswold v. Connecticut. No. 496. SUPREME COURT OF THE UNITED STATES. 7 June 1965. 27 Feb. 2007 <http://www.law.cornell.edu>.

Haggerty, Kevin D, and Amber Gazso. "The Public Politics of Opinion Research on Surveillance and Privacy." Surveillance & Society 3.2/3 (2005): 173-180 . 11 Nov. 2006 <http://www.surveillance-and-society.org/Articles3(2)/opinion.pdf>.

Hayden, Anne-Marie. “Data brokers prompt privacy concerns.” The Vancouver Sun 1 Feb. 2006: A13. LexisNexis Academic. LexisNexis. 22 Oct. 2006 <http://web.lexis-nexis.com/universe>.

- - -. “Data brokers prompt privacy concerns.” The Vancouver Sun 1 Feb. 2006, Final Edition ed.: A13.

- - -. “Two-pronged attack used to protect privacy rights.” The Star Phoenix 2 Feb. 2006: A11.

Health Insurance Portability and Accountability Act. Pub. L. 104-191. 21 Aug. 1996. A law enacted to control the health care sector in the United States, that also established some rights for patient privacy.

Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt City. No. 03-5554. SUPREME COURT OF THE UNITED STATES. 21 June 2004. 14 Apr. 2007 <http://supct.law.cornell.edu>. Petitioner Hiibel was arrested and convicted in a Nevada court for refusing to identify himself to a police officer during an investigative stop involving a reported assault. Nevada’s “stop and identify” statute requires a person detained by an officer under suspicious circumstances to identify himself. The state intermediate appellate court affirmed, rejecting Hiibel’s argument that the state law’s application to his case violated the Fourth and Fifth Amendments. The Nevada Supreme Court affirmed.

Home Page - Privacy Commissioner of Canada. 11 Mar. 2006. 5 Nov. 2006 <http://www.privcom.gc.ca/>. The home page for the Privacy Commissioner of Canada includes information about the two major pieces of Canadian Privacy Legislation as well as cases and rulings handled by the Privacy Commissioner.

House Permanent Select Committee on Intelligence. Foreign Intelligence Surveillance Act (FISA) and NSA Activities. By James X Dempsey. 2007. 18 Sept. 2007 <http://www.cdt.org>. Statement of James X. Dempsey, Policy Director, Center for Democracy & Technology. Before the House Permanent Select Committee on Intelligence Foreign Intelligence Surveillance Act (FISA) and NSA Activities September 18, 2007.

HSBCusa. HSBCusa.com Website Privacy Policy. 11 Mar. 2005. 17 Feb. 2007 <http://www.hsbcusa.com/>. The online privacy policy for HSBC USA. This privacy policy is available for viewing on the company website and only applies to transactions that occur through the website.

"Internet Privacy Policy." Verizon Wireless. 31 Jan. 2007. 17 Feb. 2007 <http://www.verizonwireless.com>.

Jacobs, Mindelle. "New Consumer Privacy Rights are on the Way." Editorial. Edmonton Sun [Alberta] 18 Nov. 2003, Tuesday Final Edition ed.: 11. 29 Oct. 2006 <http://web.lexis-nexis.com>.

JPMorgan. Privacy and Security. 2007. 17 Feb. 2007 <http://www.jpmorgan.com>. Privacy Policy for JPMorgan. No separate policy was available for Canadian customers.

Katz v. United States. No. 35. UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT. 18 Dec. 1967. 25 Apr. 2007 <http://caselaw.lp.findlaw.com>.

Kisluk, Michelle. "Canada's Privacy Commissioner Releases Decision on Outsourcing and USA Patriot Act." Mondaq Business Briefing 16 Nov. 2005: ACC-NO: 4921438.

Koontz, Linda D. “Identity Theft Issues.” House Judiciary Subcommittee: Commercial And Administrative Law. 4 Apr. 2006. LexisNexis Academic. LexisNexis. 22 Oct. 2006 <http://web.lexis-nexis.com/universe>.

Kornblutt, Anne E. “Clinton Talks of Reining In Privacy Lapses.” The New York Times 17 June 2006. 25 July 2007 <http://www.nytimes.com>.

Kurtz, Paul. “Hearing on Identity Theft/Data Broker Services.” United States Senate Committee on Commerce, Science, and Transportation. 10 May 2005. 18 Feb. 2008 <http://commerce.senate.gov>.

Kutschke, Mark. “Finds advice ‘puzzling.’” Editorial. Pembroke Observer (Ontario) 13 Nov. 2003: 4.

- - -. “Finds advice ‘puzzling.’” Letter. Pembroke Observer [Ontario] 13 Nov. 2003, Final Edition ed.: Editorial Pg. 4. Letter to the editor questions the opinion stated in a previous editorial. This letter views PIPEDA positively and states that those of the opposite opinion seek to make money by violating other people’s privacy rights.

Lawler, Barbara, and Scott Cooper. “The Opt-In Approach to Choice.” www.hp.com. 30 Jan. 2008 <www.hp.com/country/us/eng/privacy.htm>.

Lazarus, David. “Privacy policy in name only.” The San Francisco Chronicle 17 July 2005, Sunday, Final Edition ed.: E1. LexisNexis Academic. LexisNexis. 30 Nov. 2008 <http://web.lexis-nexis.com/universe>.

“Legal Notices and Privacy Statement.” Bell South. 17 Feb. 2007 <http://www.bellsouth.com>.

LexisNexis. Data Privacy Policy: Consumer Access Program. 1 Sept. 2006. 18 Feb. 2007 <http://www.lexisnexis.com>. A companion page to LexisNexis’ Privacy Policy

page. This page specifically address LexisNexis' policy of allowing customers some access to the records maintained about them.

- - -. LexisNexis Privacy Statement. 6 Mar. 2006. 18 Feb. 2007 <http://www.lexisnexis.com>. LexisNexis' online privacy policy. As with other Data Brokers, LexisNexis' privacy policy only applied to those transactions that occur between the customer and the LexisNexis website.

LexisNexis Canada. LexisNexis Canada Privacy Policy. 18 Feb. 2007 <http://www.lexisnexis.ca>. The Privacy Policy for LexisNexis Canada. LexisNexis was the only Data Broker examined that had a separate privacy policy for Canadian customers.

LICHTBLAU, ERIC. "Democrats Set to Press Bush on Privacy and Terrorism." The New York Times 7 Dec. 2006. 11 Dec. 2006 <http://www.nytimes.com>.

Long, Murray. "Nymity's President, interviews Murray Long of PrivacyScan on Canada's new Public Safety Act, 2002 and its impact on PIPEDA and organizations subject to PIPEDA. Bill C-7, the Public Safety Act, 2000, was passed on May 4 after its third reading debate in the Senate." Interview with Terry McQuay and NYMITY. NYMITY.ca. 9 Mar. 2008 <http://www.nymity.com/privaviews/2004/long.asp>. Path: ..

Lysecki, Sarah. "PIPEDA a part of doing good business: Privacy Commissioner." Computing Canada 28 Oct. 2005: 8.

MacMillan, Michael. "The biggest story of all - us." Editorial. ComputerWorld Canada 2 Jan. 2004: v.20. This piece described the current age of IT as the unruly teenage years and states that privacy laws like PIPEDA make sense for progress.

MarketResearch. MarketResearch.com Privacy Policy. 1 Sept. 2004. 18 Feb. 2007 <http://www.marketresearch.com>. Privacy Policy for MarketResearch.com

Markoff, John. "Threats And Responses: Intelligence; Pentagon Plans a Computer System That Would Peek at Personal Data of Americans." The New York Times 9 Nov. 2002. 6 Dec. 2008 <http://www.nytimes.com>.

Mastercard. Mastercard General Privacy Policy. Aug. 2004. 17 Feb. 2007 <http://www.mastercard.com>. Mastercard privacy policy. Mastercard is categorized as a member of the Financial Data Services group of companies.

- - -. Mastercard International's Canadian Online Privacy Policy. 2007. 17 Feb. 2007 <http://www.mastercard.com/canada/>. Mastercard Canada's privacy policy. Mastercard is categorized as a member of the Financial Data Services group of companies.

McCullagh, Declan. "FBI taps cell phone mic as eavesdropping tool." CNet www.news.com 4 Dec. 2006. 29 Mar. 2008 <http://www.news.com>.

McDonalds. McDonalds - Privacy Policy. 2005. 13 May 2007 <http://www.mcdonalds.com>. McDonalds U.S. Privacy Policy

McDonalds Canada. Ten Privacy Principles to be Applied to Non-Employee Information. 2008. 13 May 2007 <http://www.mcdonalds.ca>. Privacy Policy for McDonalds Canada.

McWilliams, Gary. “Minding the Store: Analyzing Customers, Best Buy Decides Not All Are Welcome; Retailer Aims to Outsmart Dogged Bargain-Hunters, And Coddle Big Spenders; Looking for ‘Barrys’ and ‘Jills.’” The Wall Street Journal [New York] 8 Nov. 2004, Eastern edition ed.: A1. ABI/INFORM. ProQuest. 29 Mar. 2007 <http://proquest.umi.com/login>.

Nantais, Chad. “Protecting our privacy.” Editorial. Windsor Star [Ontario] 11 Mar. 2005, Final Edition ed.: A9. LexisNexis Academic. LexisNexis. 29 Oct. 2006 <http://web.lexis-nexis.com/universe>.

- - -. “Protecting our privacy.” Editorial. Windsor Star [Ontario] 11 Mar. 2005, Final Edition ed., sec. Editorial/Opinion: Pg. A9. Author is a strong advocate of PIPEDA and tells readers that they should question organizations that they deal with about their Privacy Policies and practices.

“NEW Consumer Privacy Rights Are On The Way.” Editorial. Edmonton Sun [Alberta] 18 Nov. 2003, Final Edition ed., sec. EDITORIAL/OPINION: Pg. 11. Editorial describes the state of the industry as it relates to implementing PIPEDA but is happy to know that all Canadian citizens will enjoy greater privacy.

“Nextel Privacy Policy.” Sprint. 1 Sept. 2005. 17 Feb. 2007 <http://www.sprint.com>.

Nowlin, Sanford. “AT&T had plenty on its plate without privacy controversy.” San Antonio Express-News 19 May 2006, STATE&METRO Edition ed.: 1E. LexisNexis Academic. LexisNexis. 30 Nov. 2008 <http://web.lexis-nexis.com/universe>.

NYMITY Inc. 2006 Trends in Transparency. Toronto: NYMITY Inc, 2006. The report is “released in conjunction with the Canadian Marketing Association CMA) to raise

industry awareness about the importance of privacy notice transparency, and to highlight best practices adopted by many leading organizations serving the Canadian marketplace."

The Observer. "Privacy Act will impact business." Editorial. Pembroke Observer [Ontario] 30 Oct. 2003, Final Edition ed.: 4. LexisNexis Academic. LexisNexis. 29 Oct. 2006 <http://web.lexis-nexis.com/universe>.

O'Connor, Kevin. "Statement From Kevin O'Connor, CEO OF DoubleClick." www.doubleclick.com. 2 Mar. 2000. 19 Apr. 2007 <http://www.doubleclick.com>.

O'Harrow, Robert. "ID Data Conned From Firm." Washington Post 17 Feb. 2005: E01. 29 Oct. 2006 <http://www.washingtonpost.com>.

O'Harrow, Robert, Jr. No Place to Hide. New York: Free Press, 2005. A book that describes the threat to privacy in the United States. Specifically the book looks at the threat of private organizations and corporations.

Olmstead v. United States. No. 438. SUPREME COURT OF THE UNITED STATES. 4 June 1928. 13 Nov. 2008 <http://www.law.cornell.edu>. A 1928 opinion of the Supreme Court of the United States, in which the Court reviewed whether the use of wiretapped private telephone conversations, obtained by federal agents without judicial approval and subsequently used evidence, constituted a violation of the defendant's rights provided by the Fourth and Fifth Amendments. In a 5-4 decision, the Court held that neither the Fourth Amendment nor the Fifth Amendment rights of the defendant were violated. This decision was later reversed by Katz v. United States in 1967.

Patterson, Jim. “Beaudoin’s Persecution Worst Kind Of Tyranny.” Editorial. London Free Press [Ontario] 21 Feb. 2004, Saturday Final Edition ed.: F3 Letters to the Editor. LexisNexis Academic. LexisNexis. 29 Oct. 2006 <http://web.lexis-nexis.com/universe>.

- - -. “Beaudoin’s Persecution Worst Kind Of Tyranny.” Letter. London Free Press [Ontario] 21 Feb. 2004, Saturday Final Edition ed., sec. Opinion: Pg. F3Letters to the Editor. Reader found it distasteful that The Free Press would publish pictures, addresses, assessed values and personal information about the owners of “London’s 10 highest-assessed properties.” Reader is an enthusiastic advocate of PIPEDA.

Personal Data Privacy Act 2007. Pub. L. S. 495. 6 Feb. 2007. 24 June 2007 <http://www.thomas.gov>. To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

Personal Information Protection and Electronic Documents Act. Pub. L. Bill C-6. 13 Apr. 2000. The purpose of PIPEDA is to apply the same privacy controls to the private sector that already apply to the government and public sector.

Pitts, Gordon. “CIBC privacy breach sounds a general alarm.” The Globe and Mail 19 Apr. 2005, sec. REPORT ON BUSINESS: CANADIAN; PRIVACY: B4. Article discussing the Privacy Commissioner’s case of the Canadian Imperial Bank of Commerce and the leak of personal information via errant faxes.

Polonetsky, Jules. Testimony of Chief Privacy Officer at DoubleClick. Senate Committee on Commerce, Science, and Transportation. 13 June 2000. 18 Feb. 2007 <http://commerce.senate.gov>.

Ponemon, Larry. "2006 Canada 's Most Trusted Companies for Privacy Study. A privacy study conducted by Ponemon Institute and sponsored by Carlson Marketing Group." Interview with Terry McQuay and NYMITY. NYMITY.ca. 29 Aug. 2007 <http://www.nymity.ca/privaviews/2006/Ponemon.asp 1 of>.

Privacy Act. 1 July 1983. The Privacy Act protects the personal information collected by government institutions and federal works.

The Privacy Act . Pub. L. 5 U.S.C. § 552a. 31 Dec. 1974. Regulates the collection, maintenance, use, and dissemination of personal information by US federal executive branch agencies.

Privacy Act 2005. Pub. L. S. 116 . 24 Jan. 2004. 25 Jan. 2007 <http://www.thomas.gov>. To require the consent of an individual prior to the sale and marketing of such individual's personally identifiable information, and for other purposes.

"Privacy And Customer Security Policies." Verizon Wireless. Jan. 2006. 17 Feb. 2007 <http://www.verizonwireless.com>.

"Privacy at Sprint Nextel." Sprint. 2007. 17 Feb. 2007 <http://www.sprint.com>.

Privacy Commissioner of Canada. Annual Report to Parliament 2005: Report on the Personal Information Protection and Electronic Documents Act. Ottawa: n.p., 2005. The Annual Report includes a summary of the year's activity including statistics of cases handled and resolved.

Privacy Commissioner of Canada. Annual Report to Parliament 2005 Report on the Personal Information Protection and Electronic Documents Act. 2005. 5 Nov. 2006 <http://www.privcom.gc.ca/information/02_05_b_e.asp>.

- - -. Annual Report to Parliament 2004 Report on the Personal Information Protection and Electronic Documents Act. 2004. 5 Nov. 2006 <http://www.privcom.gc.ca/information/02_05_b_e.asp>.

- - -. Annual Report to Parliament 2006 Report on the Personal Information Protection and Electronic Documents Act. 2006. 5 Nov. 2006 <http://www.privcom.gc.ca/information/02_05_b_e.asp>.

Privacy Commissioner of Canada. Settled case summary #18: Business learns that it must have a privacy policy available to the public. 9 July 2006. 5 Nov. 2006 <http://www.privcom.gc.ca/ser/2006/s18_060306_e.asp>. An individual wrote to a business requesting his personal information, as well as a copy of its privacy policy. He complained that the organization not only withheld some of his personal information, but also its privacy policy.

Privacy Commissioner of Canada. Settled case summary #19: SIN not required when signing apartment lease. 9 July 2006. 5 Nov. 2006 <http://www.privcom.gc.ca/ser/2006/s19_060203_e.asp>. This case described a situation where a student's SIN (Social Insurance Number, equivalent to SSN) was requested in order to rent an apartment. The student complained to the Privacy Commissioner and the property owner agreed to change his policy.

Privacy Commissioner of Canada. Settled case summary #17: Supplementary identification required to obtain members' discount. 9 July 2006. 5 Nov. 2006

<http://www.privcom.gc.ca/ser/2005/s17_051216_e.asp>. A member of a not-for-profit association complained that he was required to show a second piece of identification, in addition to his membership card, when purchasing goods or services from the association. He thought that his membership card should be sufficient identification and that the collection of further personal information was unwarranted.

Privacy International. National Privacy Ranking 2007 - Leading Surveillance Societies Around the World. 2008. 18 Jan. 2008 <www.privacyinternational.org/survey/rankings2007/phrcomp_sort.pdf>.

"Privacy Principles." Verizon Wireless. 20 Dec. 2005. 17 Feb. 2007 <http://www.verizonwireless.com>.

The Privacy Protection Act. 19 Oct. 1980. Provides privacy protection for journalist and publications against searches by law enforcement.

Privacy Rights and Oversight for Electronic and Commercial Transactions Act of 2006. Pub. L. S.3713. 24 Sept. 2006. 24 Sept. 2006 <http://www.thomas.gov>.

Privacy Rights Clearinghouse. 11 Dec. 2006 <http://www.privacyrights.org>.

"Privacy Risk Management Solutions." NYMITY Inc. 2006. 5 Nov. 2006 <http://www.nymity.com/>. Nymity, Canada's leading privacy research firm, provides pragmatic management support solutions that help organizations manage the risks that lead to a data breach, a privacy complaint and to non-compliance or over-compliance with privacy laws.

"Privacy Statement." Comcast. 1 July 2004. 17 Feb. 2007 <http://www.comcast.com>.

"Protecting your privacy." Editorial. The Leader-Post [Regina] 15 Mar. 2004, Monday Final Edition ed., sec. Viewpoints; Our View: Pg. B7. Describes PIPEDA as a huge issue that has gone unnoticed by far too many people. The authors says that privacy is a critical issue for everyone.

Public Safety Act. 29 Apr. 2002. Designed to improve the legislative framework in order to fight terrorism and protect public safety.

Rachels, James. "Why Privacy is Important." Philosophy and Public Affairs 4.4 (1975): 323-333. JSTOR. 13 Nov. 2006 <http://www.jstor.org/search>.

Rahn, Richard W. "Drifting from freedom." The Washington Times 30 Jan. 2005: B03. 29 Jan. 2007 <http://www.washingtontimes.com/>.

"A Review of the Fair Information Principles: The Foundation of Privacy Public Policy." The Privacy Rights Clearinghouse. Feb. 2004. 2 May 2007 <http://www.privacyrights.org/ar/fairinfo.htm>.

Roe v. Wade. No. 70-18. SUPREME COURT OF THE UNITED STATES. 22 Jan. 1973. 5 Aug. 2007 <http://www.law.cornell.edu/>.

Rotenberg, Marc. "Identity Theft and Data Broker Services." Committee on Commerce, Science and Transportation, United States Senate. 10 May 2005. 18 Feb. 2007 <http://commerce.senate.gov>.

Rothfeder, Jeffrey. Privacy for Sale: How Computerization has made Everyone's Life an Open Secret. N.p.: Simon & Schuster, 1992.

Sahadi, Jeanne. "Privacy experts' wish list If privacy advocates had their way, consumers would gain far more control over their information." CNN.com 13 May 2005. 13 Nov. 2006 <http://www.cnn.com>.

Samel, Shelley. “Privacy law: what you need to know.” Editorial. Brunico Communications 15 Dec. 2003: 11. LexisNexis Academic. LexisNexis. 29 Oct. 2006 <http://web.lexis-nexis.com/universe>.

- - -. “Privacy law: what you need to know.” Strategy 15 Dec. 2003: Pg. 11. Provides a summary of PIPEDA for a sector of industry.

Schmitt, Richard B. “The Nation; FBI has some explaining to do; Senators question the bureau’s director about abuses of power. He urges them not to gut a Patriot Act provision.” The Los Angeles Times 28 Mar. 2007, Home Edition ed.: 12. LexisNexis Academic. LexisNexis. 6 June 2007 <http://web.lexis-nexis.com/universe>.

Schwartz, Ari. “Reauthorization of the Federal Trade Commission.” Senate Committee on Commerce, Science, and Transportation Subcommittee on Interstate Commerce, Trade and Tourism. 12 Sept. 2007. 12 Nov. 2007 <http://commerce.senate.gov>.

Senate Committee on Commerce, Science, and Transportation. Reauthorization of the Federal Trade Commission. By Ari Schwartz. 2007. 23 Sept. 2007 <http://www.cdt.org>. Testimony of Ari Schwartz, Deputy Director Center for Democracy and Technology before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Interstate Commerce, Trade and Tourism on “Reauthorization of the Federal Trade Commission” September 12, 2007.

Silva, Jeffrey. “Fine ‘merely cost of doing business,’ Martin laments; FCC levies $97,500 fine on data broker.” RCR Wireless News 17 July 2006: 11. LexisNexis Academic. LexisNexis. 30 Nov. 2008 <http://web.lexis-nexis.com/universe>.

Silverman v. United States. No. 505. U.S. Supreme Court. 6 Mar. 1961. 25 Apr. 2007 <http://caselaw.lp.findlaw.com>.

Smith, Gordon. "Hearing On Federal Solutions to Data Breach and Identity Theft." Senate Subcommittee on Trade, Tourism, and Economic Development Senate Committee On Commerce, Science, And Transportation. 16 June 2005. 18 Feb. 2007 <http://commerce.senate.gov>.

Sorrell, William H. "Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use." United States Senate Committee on the Judiciary. 13 Apr. 2005. 18 Feb. 2007 <http://judiciary.senate.gov>.

"Sprint Nextel Sues to Shut Down Online Services That Illegally Obtain and Sell Confidential Telephone Records; Lawsuit Aims to Protect Customer Privacy by Eliminating Fraudulent Activities of Online Data Brokers." Business Wire 27 Jan. 2006. LexisNexis Academic. LexisNexis. 1 Apr. 2007 <http://web.lexis-nexis.com/universe>.

"Sprint Privacy Policy." Sprint. 1 Sept. 2005. 17 Feb. 2007 <http://www.sprint.com>.

SRA International. SRA International - Legal & Privacy. 2007. 18 Feb. 2007 <http://www.sra.com>. SRA International's online privacy policy. As with other Data Brokers, SRA International's privacy policy only applied to those transactions that occur between the customer and the SRA International website.

Stalking Is A Crime Called Criminal Harassment. Ottawa: Department of Justice Canada, 2003.

State Farm. State Farm - Our Privacy Principles. 2006. 13 May 2007 <http://www.statefarm.com>. State Farm U.S. privacy policy. State Farm is categorized as a member of the Insurance group of companies.

State Farm Canada. State Farm Privacy Notice. 13 May 2007 <http://www.statefarm.ca>. State Farm Canada's privacy policy. State Farm is categorized as a member of the Insurance group of companies.

Stoddart, Jennifer. Senate Standing Committee on Transport and Communications. 18 Mar. 2004. 3 Jan. 2009 <http://www.privcom.gc.ca>.

- - -. "A look back at PIPEDA." Editorial. Canadian HR Reporter 19 June 2006: 19. ABI/ INFORM. OCLC. 15 Oct. 2006 <http://firstsearch.oclc.org/>.

- - -. Stoddart Testimony Regarding Public Safety Act, 2002. Senate Standing Committee on Transport and Communications. Ottawa Ontario. 18 Mar. 2004. 5 Nov. 2006 <http://www.privcom.gc.ca/speech/2004/sp-d_040318_e.asp>. Privacy Commissioner describes Public Safety Act as blurring the line between the public and private sectors. Ms. Stoddart's concerns stem from amendments that allow private firms to collect information on behalf of national security agencies.

Stokey, Edith, and Richard Zeckhauser. A Primer for Policy Analysis. New York: W. W. Norton & Company, Inc, 1978. This book provided a framework of policy decision making and possible policy solutions. Part III of the Book, Ends and Means (p. 256) was particularly helpful.

Subcommittee on Commercial and Administrative Law and The Subcommittee On The Constitution Of The Committee On The Judiciary House Of Representatives. Personal Information Acquired By The Government From Information Resellers: Is There Need For Improvement? Washington D.C., 2006. 13 Nov. 2006 <http://judiciary.house.gov/>.

Sullivan, Michael. "Privacy Solutions for Direct Marketing." Interview with Terry McQuay and NYMITY. NYMITY.ca. 8 July 2007 <http://www.nymity.com/privaviews/2007/Sullivan.asp>. Path: ..

Sungard. Sungard Privacy Policy. 2003. 17 Feb. 2007 <http://www.sungard.com>. Sungard privacy policy. Sungard is categorized as a member of the Financial Data Services group of companies.

Swartz, Nikki. "No Respect for PIPEDA." Information Management Journal (Sept.-Oct. 2006): 21.

Swecker, Chris. "Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use." United States Senate Committee on the Judiciary. 13 Apr. 2005. 18 Feb. 2007 <http://judiciary.senate.gov>.

Swire, Peter. "Consumer Privacy." House Energy And Commerce Subcommittee: Commerce, Trade, And Consumer Protection. LexisNexis Academic. LexisNexis. 22 Oct. 2006 <http://web.lexis-nexis.com/universe>.

TacoBell. TacoBell - Privacy Policy. 11 July 2006. 13 May 2007 <http://www.tacobell.com>. Privacy Policy for TacoBell Canada

TacoBell Canada. TacoBell - Privacy Policy. 1 Sept. 2006. 13 May 2007 <http://www.tacobell.ca>. Privacy Policy for TacoBell Canada

The Observer. “Privacy Act will impact business.” Editorial. Pembroke Observer [Ontario] 30 Oct. 2003, Final Edition ed., sec. EDITORIAL: Pg. 4. Author views PIPEDA as the efforts of “Big Brother” and believes it will have a very negative impact on small businesses.

Ticketmaster. Ticketmaster.com Privacy Policy. 8 Oct. 2006 <http://www.ticketmaster.com>. Privacy Policy for Ticketmaster.com

Tracked, Profiled, and Identified: Privacy and the Linkage of Data to Individuals. AALS, 2006. Association of American Law Schools AALS. 18 Oct. 2007 <http://www.aals.org/am2006/program/friday.html>. Covers issues of how data is connected to people, how Radio Frequency Identification (RFID) and other identification techniques may be able to better link data to people, and how the data is used to make decisions about them.

Travelocity. Privacy Policy. 13 May 2007 <http://www.travelocity.ca>. Privacy Policy for Travelocity Canada.

- - -. Privacy Policy. 15 Apr. 2007 <http://www.travelocity.com>. Privacy Policy for Travelocity US.

Traver, C. Privacy, Law and the Human Genome Project: A Review of the Literature 1968-1993. N.p.: Center for Social and Legal Research, 1995. This report discussed the piecemeal approach of American privacy legislation

Trotta, Daniel. “Rights group requests wiretapping probe.” Reuters 24 May 2006. 22 Oct. 2007 <http://www.reuters.com>.

Turow, Joseph, and Chris Jay Hoofnagle. The FTC and Consumer Privacy in the Coming Decade. 2006. 4 Apr. 2007 <http://repository.upenn.edu/cgi/viewcontent.cgi?article=1066&context=asc_papers>.

Urquhart, Ian. "Tories drag feet on privacy policy." Editorial. The Toronto Star [Toronto] 23 June 2003, Monday Ontario Edition ed., sec. OPINION: Pg. A21. The author is critical of the Tories party and how slow they have been to implement privacy legislation in Ontario prior to the July 1 implementation date of PIPEDA. The author believes that implementing their own provincial law would protect them from some of the less favorable terms in PIPEDA.

USBC Canada. HSBC Privacy Code. 1 Jan. 2004. 17 Feb. 2007 <http://www.hsbc.ca>. Privacy policy for HSBC Canada. The document is a 16-page PDF available for download on the companies website. Contains HSBC Canada's privacy principles for how it collects and handles consumer information.

U.S. Census Bureau. Top Ten Countries with which the U.S. Trades For the month of December 2007. 8 Mar. 2008 <http://www.census.gov/foreign-trade/top/dst/2007/12/balance.html>.

U.S Department of Health, Education and Welfare. Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. 1973. 4 Apr. 2007 <http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>.

"Verizon Wireless Continues Campaign To Defend Customers' Privacy With Legal Action Against Two Telemarketers; First Lawsuit to Allege Telemarketing Firm Spammed Verizon Wireless Customers with Spanish-language Calls." PR Newswire US 14 Feb. 2006. LexisNexis Academic. LexisNexis. 1 Apr. 2007 <http://web.lexis-nexis.com/universe>.

Vertis Communications. Vertis Communications : Privacy Policy. 2007. 18 Feb. 2007 <http://www.vertisinc.com>. Privacy Policy for Vertis Communications.

"Visitor Agreement." Comcast. 1 July 2004. 17 Feb. 2007 <http://www.comcast.com>.

Wachovia. Wachovia Privacy Statement. Jan. 2007. 17 Feb. 2007 <http://www.wachovia.com>. Privacy Policy for Wachovia bank. No separate privacy policy was available for Canadian customers.

Walmart. Wal-Mart Stores, Inc. Privacy Policy for Customers and Members . 27 Apr. 2007. 30 Sept. 2007 <http://www.walmart.com>. Privacy Policy for Walmart U.S.

Walmart Canada. Walmart Canada Corp. Privacy Policy. 1 Jan. 2004. 30 Sept. 2007 <http://www.walmart.ca>. Privacy Policy for Walmart Canada.

Warren, and Brandeis. "The Right to Privacy." Harvard Law Review IV.5 (1890). 11 Sept. 2005 <http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html>.

Wearden, Graeme. "U.S. tech protests EU privacy laws." ZDNet (UK) 30 Sept. 2002. 5 Nov. 2006 <http://news.zdnet.com>.

Wells Fargo. Online Privacy Policy. 30 Nov. 2006. 17 Feb. 2007 <http://www.wellsfargo.com>. U.S. Privacy Policy for Wells Fargo bank. A separate privacy policy was available on another site for Canadian customers.

- - -. Privacy Policy for Individuals. 1 Jan. 2007. 17 Feb. 2007 <http://www.wellsfargo.com>. A companion website to Wells Fargo's U.S. Privacy Policy. A separate policy was available for Canadian customers.

Wells Fargo Canada. Summary of the Code for the Protection of Personal Information. 17 Feb. 2007 <http://financial.wellsfargo.com/canada/en/index.html>. A PDF document available for download that provides a summary of Wells Fargo Canada's handling of customer personal information.

Westin, Allen F. Privacy and Freedom. N.p.: Atheneum, 1967.

Wunsch, Charles. "Unauthorized Information Collection Using Pretexting." Committee: House Energy and Commerce. 29 Sept. 2006. LexisNexis Academic. LexisNexis. 1 Apr. 2007 <http://web.lexis-nexis.com/universe>.

Zuckerman, M.J. "Computer crimes surge Companies fear losing privacy, customers' trust." USA TODAY 2 July 1996: 1A. ABI/INFORM. ProQuest. 1 Apr. 2007 <http://proquest.umi.com/login>.