2006

Privacy Policies: A Study of Their Use Among Online Canadian Pharmacies

Joanne Kuzma
Nova Southeastern University, jmk6281@aol.com

Privacy Policies: A Study of Their Use Among Online Canadian Pharmacies

By

Joanne Kuzma

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy

Graduate School of Computer and Information Sciences
Nova Southeastern University

2006

We hereby certify that this dissertation, submitted by Joanne Kuzma, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

_____ _____

Steven D. Zink, Ph.D. Date
Chairperson of Dissertation Committee

_____ _____

Maxine S. Cohen, Ph.D. Date
Dissertation Committee Member

_____ _____

William L. Hafner, Ph.D. Date
Dissertation Committee Member

Approved:

_____ _____

Edward Lieblein, Ph.D. Date
Dean

Graduate School of Computer and Information Sciences
Nova Southeastern University

2006

An Abstract of a Dissertation Submitted to Nova Southeastern University
In Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy

Privacy Policies:
A Study of Their Use Among Online Canadian Pharmacies

by
Joanne Kuzma

August 2006

The use of online Canadian pharmacies has grown over the past decade due to lower cost medications and ease of use. In order for these firms to gain business and marketing information, they collect a variety of consumer data. This has raised concerns among consumers as to privacy issues of the data collected by these online firms. However, researchers have not effectively examined how online consumers value specific privacy factors when deciding whether to use the sites. Also, studies have not determined if many of these sites have comprehensive privacy policies that indicate if they protect consumers' data for a variety of factors. This research included a study of 25 major online Canadian pharmacies to determine the completeness of privacy policy factors among this population. This survey showed the majority of sites did contain a privacy policy. However, the comprehensiveness of policies differed vastly among the sites. This dissertation also included an investigation of consumers' views of the privacy policy factors they feel are important when deciding to use these pharmacy sites. Results of a survey of 147 users of medical Web sites showed that consumers were concerned about privacy on these sites, with opt-in, security and consumer/licensing issues of high importance. However, the study also showed that for consumers who actually used an online pharmacy during the past year, cost savings, rather than privacy issues were the principal concern. This dissertation created an instrument that online firms can use to evaluate consumers perceptions of privacy policies, as well as which policies are important to include on a Web site.

Acknowledgements

My heartfelt thanks goes to all those who assisted me with this project. I thank Dr. Steven Zink for his brilliant proofreading and continued assistance in making completion of this dissertation possible. I also thank my committee members, Dr. Maxine Cohen and Dr. William Hafner, for their valuable input.

I also acknowledge by employer, St. Petersburg College, whose faculty helped with suggestions on how to proceed with the study and survey. I thank the students in my electronic commerce class for serving as guinea pigs for the initial survey.

To my parents, thanks for your support and patience during this process.

Table of Contents

List of Tables

Tables

Chapter 1

Introduction

In a decade, consumer pharmaceutical sales have evolved from solely a brick-and-mortar business to one involving the ability to order prescriptions via Internet-based firms. Part of this industry also involves the rise of so-called “Canadian pharmacies” -- Web sites that offer American consumers the ability to purchase pharmaceuticals shipped from Canada, usually at substantially reduced prices compared to prescriptions obtained through traditional U.S. pharmacies.

Online businesses have gathered a rich amount of data about their customers for marketing purposes and this growth of information has allowed the firms to better target their audience and marketing efforts to gain new clientele. However, it has also created concerns among online consumers who are apprehensive with the amount of data collected, especially without their consent (Rose, 2000). This apprehension extends to consumers in the online pharmacy realm. The increasing use of online pharmacy sites and other commercial sales have necessitated governments adopting privacy laws, as well as individual sites adopting comprehensive policies to protect consumer information. An industry research firm, PharmacyChecker.com (2003a), notes that there is currently inadequate protection of online consumers and that in 2003, 70% of the online American and Canadian pharmacies did not provide adequate security and privacy of a customer's personal and financial information.

This dissertation research evaluated the effectiveness of privacy protection among various online Canadian pharmacy Web sites. Because of the rise in consumer awareness

of privacy issues as well as the increase in Americans utilizing Canadian pharmacies, it is helpful for consumers to understand which sites are meeting legal requirements and industry guidelines for posted privacy statements. This study also examined other factors that played a role in consumers' usage of these sites, such as if they viewed licenses, security features, and data sharing in a positive or negative light.

Problem Statement

Some Canadian online pharmacies may not meet American or Canadian privacy laws and may not provide adequate privacy protection to their clientele. Non-adherence to regulation or lack of consistent policies among the myriad of online pharmacy sites can result in lack of secure private consumer information, consumer confusion about drug information, and the possibility of third party organizations' purchase of consumers' data. For those sites with policies, a key question asked was if the main elements in their policies are stated in such a way that they effectively adhere to legal requirements and address consumers' privacy concerns.

Goal

An investigation of 25 major online Canadian pharmacies (see Appendix A) determined how well these sites support industry guidelines. It was important to understand how well the average site follows privacy guidelines, as this can affect consumers' perceptions and usage of a specific site. In addition, the research included a survey of Canadian online pharmacy users and reviewed their experiences and attitudes towards conducting purchases on these sites to determine if privacy issues are a major concern.

There were four facets to this study. The first was developing a framework of analysis to determine if the sites adhered to legal privacy regulations. The second part was analyzing statistical differences in privacy policies among 25 major online Canadian pharmacy sites among the hundreds available on the Web. Third, the study determined the comprehensiveness of privacy policies for Canadian online pharmacies. A pharmacy site that scored well on the statistics gathered in the study can be considered highly effective in promoting customer privacy and adhering to privacy laws and guidelines. Finally, consumer views towards the use of these sites were analyzed to determine if privacy issues were a major concern when conducting business on these pharmacy sites. The product of this study is a model that can be used to evaluate the effectiveness of privacy policies, not only for Canadian pharmacies, but perhaps also for a myriad of other online, e-commerce firms.

Twenty-five online pharmacies provided an adequate sample to analyze privacy policy issues. The researcher chose the 25 pharmacies from an online search of Google.com. In addition to an analysis of these sites, a survey of 147 users of several medical sites was conducted. A link to an online research questionnaire was posted on several consumer medical information sites in order to assess consumer purchasing patterns and viewpoints.

Research Questions

In this study of the use of privacy policies among Canadian online pharmacies, the following research questions were addressed:

1. What types of privacy issues do Canadian online pharmacies address?

2. Do gaps exist in privacy protection provided to consumers of online Canadian pharmacies?
3. Which online pharmacies offer the most comprehensive privacy policies and what are their strengths and weaknesses?
4. What privacy and non-privacy criteria do consumers use when deciding to order from these sites, and what factors do non-buyers cite for not purchasing drugs?

Relevance and Significance

Relevance

The research in this area is relevant for several reasons. There has been a lack of scholarly study addressing the issue of privacy policies among Canadian online pharmacies. Several research papers have analyzed the results of studies performed on a number of general Web sites with posted privacy policies, but none has accomplished an in-depth review of only online Canadian pharmaceutical firms. A U.S. Federal Trade Commission (FTC) study of American sites found that although 99% of general sites collected personal information in 2000, only 20% of a random sample and 42% of the most popular sites routinely observed fair information practices (overall guidelines to which firms should adhere when conducting business) ("Online Privacy," 2000). A more recent study based on the FTC's methodology was conducted in December 2001. The researchers analyzed 85 of the busiest Web sites and found that sites were collecting less information in 2001 than in prior years. They also found that fewer Web sites were utilizing third party cookies, privacy notices were more prevalent and complete, and more sites offered opt-in rather than opt-out options (Adkinson, Eisenach, & Lenard, 2002).

There is a lack of comprehensive empirical research examining privacy issues as they relate to online Canadian firms. PharmacyChecker.com (2003a) completed a study of 20 online Canadian pharmacies. They based their study on the first 20 Canadian online firms found on a search of Google. Their study found 70% of these firms were deficient in protecting privacy or offering secure transactions. Most of the sites that met their criteria for good privacy protection in their posted policies were online extensions of existing licensed pharmacies. The study found a wide variety in privacy policies and terms offered to consumers. However, their study was based on limited research questions and methods when collecting information and analyzing the results. Three relevant categories of privacy features were reviewed when compiling their results: (a) company address and phone number provided, (b) promises of privacy of personal/medical information, and (c) financial information sent online is secure (PharmacyChecker.com, 2003c). Because of the limited information collected and the lack of reliable research instrument modeling, that study was limited in its scope and findings.

Dixon (2003) completed a study of 53 job search sites to review how each site operates relative to consumer privacy information. She conducted a more comprehensive review of privacy policy issues than the limited PharmacyChecker study, although this study was limited to the online employment search industry. While her study concentrated on privacy issues with online job search sites, some of her analysis can be applied to studies of online Canadian pharmacies. For example, online firms of any industry, not just the online employment arena, can use cookies, opt-in, opt-out, trust and seal programs, and security of customer information and transactions.

The study is also relevant because the number of online pharmaceutical firms and customers using these sites is increasing every year. Online consumers are becoming more sophisticated in Internet ordering, and have an increased awareness of online privacy issues. They want the option of using sites that have acknowledged and easily understood privacy policies. However, although they may desire high levels of privacy, other factors, such as low-cost pharmaceutical products may override privacy concerns.

Significance

This dissertation will advance the area of privacy analysis of this industry by providing a research methodology for analyzing privacy policies. This study is geared towards a review of these issues among Canadian online pharmacies, but the methods could be expanded to encompass an analysis of other online industries. It introduces survey techniques and questions to aid researchers in effectively appraising consumers' views on using these sites.

Barriers and Issues

To date, the goal of this study had not been met for a number of reasons. First, although Canadian law may specify that sites must adhere to privacy regulations, the rapid increase in the number of Web sites in this industry results in some sites not understanding or adhering to all legal requirements. Large firms with budgets and time to keep current with policies may have them posted on their Web site. Smaller firms may either not be aware of guidelines or do not have the budget to adhere to them. In addition, unethical firms likely have no desire to implement policies. Leizerov (2001) also states that the rapid technological development of the Internet has presented an impediment to

creating a framework for coherent rules, which could make it difficult for firms to stay abreast of legislation or industry guidelines and best practices.

Although U.S. consumers enjoy considerable savings by using Canadian online pharmacies, the practice of purchasing drugs from Canada and importing them to the U.S. is illegal under U.S. law. Thus, consumers may not wish to complain if they encounter problems with these firms. In addition, this industry has attracted many new firms over the past several years, and not all these pharmacies are licensed in Canada. It should be noted that some of these Web sites may promote themselves as "online pharmacies," but may merely be administrative or marketing corporations affiliated with either licensed or unlicensed Canadian pharmacies. PharmacyChecker.com (2003b) has studied Canadian online pharmacies and estimated that 50% do not hold valid Canadian pharmacy licenses. This could lead to problems with wrong medication, fake drugs, or poor service. These concerns, combined with lack of effective privacy policies, could heighten trepidations consumers have with these organizations.

Another barrier to the study was the rapid proliferation of online pharmacies in order to meet the rising demands of consumers looking for affordable medication. Jupiter Research indicates that Canadian online pharmaceutical sales doubled to $584 million from 2002 to 2004 (IMS Health Canada, 2005). As the number of online pharmacies and sales increases, it becomes difficult to monitor the growing number of firms and their privacy policies.

Approach

The research was accomplished through the analysis of 25 online Canadian pharmacy sites to determine what privacy policies they were following. First, best-practice privacy policies and legal requirements were gathered to determine what specific guidelines online sites should follow. Next, a data gathering review determined what specific guidelines were used at each site, as well as those that were not included on the policy page. Then, a questionnaire was compiled for users who frequented online medical sites to assess their experiences and feelings of Canadian online sites.

The completed study included the following:

1. List of major general and industry-specific privacy policies that can be included on Canadian pharmacy Web sites. The literature review aided in the development of the research questions to compile in the site surveys. A number of general privacy policy provisions that should be contained on any Web site were included, as well as specific policies for the online pharmacy industry. Some of these factors included: (a) privacy seal usage, (b) demographic and personal information, (c) medical data, (d) use of cookies, (e) profiling information, (f) opt-in and opt-out abilities, (g) ability for users to update personal information, (h) disclosure of information to third-party firms, (i) security protection, (j) collection of data from children under 13 years of age in compliance with the Children's Online Privacy Protection Act (COPPA) law, (k) posting changes to privacy policies on the site, (l) email or phone contact on the

privacy page, and (m) pharmacy licensing and prescription requirements on the site.

2. Compilation and analysis of Canadian (federal and provincial) and American (federal and state) privacy laws. Legal considerations were important in analyzing which sites follow regulations and to what degree these laws are being adhered.
3. Selection of 25 online Canadian pharmacy sites chosen from two listings to analyze their privacy policies. Half of the pharmacy list was compiled randomly from the Canadian Online Pharmacy Directory (2004), an online Web site service that aides U.S. citizens in locating Canadian online pharmacies. The other portion of the list was gathered from a search of Google.com. From these two sources, a final list of 25 Canadian pharmacies was used for research on specific privacy policy issues. These sites are included in Appendix A.
4. Analysis of each of the 25 sites to determine if they meet privacy policies in relation to legal and best-practice requirements, as well as to identify potential gaps. This was accomplished by examining the privacy policy page for each site. A manual inspection of each page determined if specific privacy factors were listed on the site, or whether the site included those features.
5. Administration of a survey questionnaire for Internet users to determine their views on Canadian online pharmacies. This survey consisted of a series of questions and was hosted on an online site through

www.hostedsurvey.com. Some questions consisted of demographics, site usage, and perception queries. Age and gender demographic inquiries determined the type of users who normally utilize these sites. Other questions established which factors were important to consumers when they choose which sites to use. This information will be beneficial to online Canadian pharmacies to determine how important privacy issues are to the consumers versus other factors, such as cost or convenience.

6. Selection of online medical information sites that were used to create links to the survey. In order to find a significant statistical survey of respondents who utilize Canadian online pharmacies, it was imperative to select one or more general medical information sites where the readers would be inclined to need prescriptions, and thus use pharmacies to fill their pharmaceutical needs. Of the respondents to the survey, it was anticipated that some of them would have used Canadian sites. For those who did not use online pharmacies, the survey questions queried why they did not, such as concerns with privacy policies or legal issues.
7. Query of online users and analyzed the results. Statistical techniques were defined to analyze the raw data. This included both an initial testing group of 10 students and a final group of 147 consumers.

Resources

Accomplishing the objectives for this study required analyzing 25 online Canadian pharmacies that cater to U.S. consumers. The researcher reviewed both licensed as well as unlicensed firms. Many of the so-called “Canadian pharmacy” Web sites are

not truly licensed pharmacies, and merely function as facilitators between online customers and traditional pharmacies. However, many operate under the guise of legitimate pharmacies, and are often financially successful. Therefore, it was imperative to study both legitimate, licensed firms as well as unlicensed sites.

A Web-based survey allowed for analysis of perceptions about Canadian pharmacies. The audience consisted of U.S. consumers who utilized medical information sites and were willing to take an online survey. The study analyzed both users and non-users of online Canadian pharmacy sites to determine which factors (privacy policies, cost, quality, etc.) consumers found the most influential in their choice of sites.

Chapter 2

Literature Review

Introduction

The growth of Canadian online pharmacies is a phenomenon resulting from the price differential between American and Canadian prices for medication. Lack of insurance and high prices for pharmaceuticals have resulted in many American consumers bypassing U.S. pharmacies for the lower-priced Canadian market. PharmacyChecker.com, an independent research firm, collects and analyzes online pharmacy data. They indicate that because of Canadian price controls on drugs, pharmaceuticals sold in Canada are, on average, 50% lower in cost than the same drug in the U.S. (PharmacyChecker.com, 2003e). The savings have attracted U.S. consumers to these sites, but the migration has not come without controversy, such as lack of consistent and comprehensive privacy policies.

According to data from IMS Health, a company that studies the pharmaceutical market, Americans fill over three billion prescriptions annually, generating over $200 billion in revenues (Fox, 2004a). She indicates chain stores account for the largest segment of pharmacy sales (36.2%), followed by independent drug stores (14.4%), and mail order services (13.8%). Currently, only 4% of all U.S. pharmacy consumers have purchased prescription drugs online. Concern about disclosing personal information online is a concern for consumers across retail sectors (Resnick & Montania, 2003). Privacy concerns make online disclosure of medical information an especially sensitive

issue to online consumers (Choy, Hudson, Pritts, & Goldman, 2001). In addition, consumers express apprehension about the quality of prescription drugs purchased online, particularly if the pharmacies are not licensed in the United States and thus not subject to U.S. safety and quality standards (Fox, 2004a).

With poor online privacy practices, many companies will experience negative effects not only on their online sales, but also in a shift of customers to more privacy-sensitive competitors (Dienekis Information Systems, 2004). It would follow that online service firms might alleviate customers' concerns by developing and posting a comprehensive privacy policy on their Web sites.

Political Issues with Online Pharmacies

Pharmaceutical prices in the U.S. far exceed those of most other Western nations, and U.S. consumers find that they are often unable or unwilling to pay the established prices (Cohen, 2004). Additionally, in 2004, 15.7 percent of the American population lacked insurance to cover prescription drug costs (U.S. Census Bureau, 2005) and the option of purchasing lower-cost drugs from foreign firms becomes attractive. Unlike the U.S., some foreign countries set maximum prices for pharmaceuticals in order to make them affordable for their citizens. For example, Canada has a federal board that sets price ceilings on drugs (Krauss, 2004; Parloff, 2004). The purchase of drugs from Canadian pharmacies over the Internet has become a topic of heated debate that extends to the U.S. Congress and state legislatures. The governors of Illinois, Minnesota, New Hampshire, and Wisconsin have established online directories of recommended Canadian pharmacies (Fox, 2004a). The governors of Iowa, Maine, Michigan, Ohio, Vermont, and West Virginia have expressed similar interest in providing their residents with online access to

Canadian pharmacies (Korcok, 2004). Michael Albano, mayor of Springfield, Massachusetts took the initiative in arranging for Springfield's 9,000 municipal employees to purchase drugs from a designated Canadian pharmacy at an estimated cost savings of $4 million to $9 million annually (Korcok, 2004). As of December 2003, about 3,300 employees had used the program, saving the city roughly $1 million (Parloff, 2004). The average savings to U.S. consumers is substantial. The U.S. Senate Subcommittee on Consumer Affairs, Foreign Commerce, and Tourism reviewed a study by the United Health Alliance, a nonprofit physicians' health group. A study of 145 U.S. senior citizens showed that U.S. citizens paid $81,000 for their prescriptions in the U.S. and only $22,000 for the same prescriptions in Canada (U.S. Congress, Senate, 2001).

Both the pharmaceutical industry and the U.S. Food and Drug Administration (FDA) have expressed powerful opposition to U.S. citizens purchasing Canadian pharmaceuticals because they cannot guarantee the safety of drugs imported from outside the U.S. (Hubbard, 2003; Meadows, 2002). Advocates counter that their motives are based on economic factors and profits rather than on safety concerns (Cohen, 2004). Alternately, opponents of Canadian drug importation have accused some Canadian Internet pharmacies of the same profit motive (Whitbaum, 2003).

The "political gridlock" over extending prescription drug benefits to Medicare beneficiaries generated "anger and despair" among older adults and many have difficulties paying for needed drugs (Korcok, 2002, p. 1). In 2002, Congress failed to pass a proposed measure that would ease access to the re-importation of cheaper prescription drugs from Canada. Noting that the government covers 75% of prescription drug costs for congressional members, Senator Edward Kennedy (D-MA) spoke out,

"How many of us are willing to face our constituents… knowing that we have secure coverage…but we reject proposals that do even less for our fellow citizens?" (Korcok, 2002, p. 1). Parloff (2004) stressed that support for legalizing access to Canadian pharmacies is not a partisan issue.

Consumer Economic Issues

The dispute over purchasing drugs from online Canadian pharmacies may be rooted in a variety of issues related to e-commerce practices and how the online pharmacy industry operates in the context of the global online economy, especially the legal and moral aspects related to privacy. There are differences and similarities in both the privacy policies and pharmacy regulations of the U.S. and Canada. To many people, cyberspace is a vast entity that allows them anonymous exploration with an assumption their surfing habits and information is protected. However, the existence of cookies and Web bugs (clear gifs) belies any assumption that online browsing is really anonymous (Olsen, 2000). On the contrary

> Every time an individual interacts with the Web, she or he leaves behind a trail of extraordinary detailed information about their identity, preferences, hobbies, buying habits, financial status, and even medical records. This private information of customers can be—and actually is—used and abused (Reisch, 2003, p. 103)

Regarding the issue of consumers providing their personal information to online health sites, Choy et al. (2001) stated, "The potential for abuse is enormous" (p. 25). Consumers engage in a cost-benefit analysis when they decide to purchase online. On one side are their concerns with privacy and security; on the other side are factors such as convenience, cost, and 24-hour access. Adults who have used the Internet for finding

health information or buying health-related products (including prescription drugs) acknowledge the legitimacy of arguments on both sides (Fox & Rainie, 2000). The decision that the benefits outweigh the potential costs of making a purchase online is typically based on consumers' perceptions that the vendor will treat them fairly (Pennington, Wilcox, & Grover, 2003). Visible signs such as privacy seals, guarantees, and customer ratings enhance consumer's perceptions of trust of Internet sites (Pennington et al., 2003).

Reisch (2003) outlined the potential benefits and pitfalls of online commerce for consumers. The benefits of online shopping include:

- *Lower transaction costs* with respect to time, money, and access to product-related information and services.
- *Lower costs of consumer organization,* including the potential for networking, strategic alliances, virtual consumer organizations, information access and transparency, power shopping, comparison shopping, price agents, and consumer platforms.
- *Entertainment and stimulation* due to the interactive nature of the medium.
- *Individualization* in the form of customized information and advertisements.

Reisch (2003) notes that, "While these promises are intriguing, there is a dark side to Internet technology usage" (p. 99). Two of the "dark" factors she mentions are relevant to this study privacy and security. She states

> The *privacy of consumer information* that is collected for commercial purposes is seen as a distinct consumer right from both legal and ethical perspectives, and the

> secure storage and transmission of consumer information is regarded as an integral step in maintaining that privacy. (Reisch, 2003, p. 99)

However, the vast amount of information stored in business databases, combined with lack of national privacy legislation, inconsistent self-regulation of online firms, and consumers' lack of understanding about protection of their private information contribute to the risk of breaches of consumer privacy. Reisch (2003) states, "it is not usually the disclosure of data that is problematic, so long as it is provided voluntarily and as long as users are made fully aware of how this information is going to be used" (p. 100). The disclosure of information is often mandatory if customers want to use online sites and complete electronic transactions. However, serious privacy problems can arise when the information is shared with business affiliates outside the control of the host Internet site.

Howard Beales (2002) states that the focus of consumer privacy protection should be on "*misuse* of information" (p. 1). Whereas data collection had been the previous focus of the FTC's Bureau of Consumer Protection, the current focus is on preventing the abuse and misuse of information that has been voluntarily disclosed.

Beales (2002) describes the FTC's 2002 privacy agenda involving pharmaceutical manufacturer Eli Lilly and Company. The complaint presented to the FTC alleged that Lilly did not take appropriate actions to protect the security and confidentiality of information provided to Lilly.com and Prozac.com. The result was that Lilly inadvertently disclosed the e-mail addresses of 669 visitors to those sites. Underscoring the privacy concerns of consumers who use the Web for health information and drug purchases, Beales noted, "This was very sensitive information, where release could have serious adverse consequences for the consumer involved" (p. 2).

Another issue related to privacy abuse, can occur when companies violate their own privacy policies. McCullagh (2004) iterates that although consumers may research a site's policies, this action becomes questionable if the online firm does not adhere to the stated policies. Not only does this problem occur with private industry, but it also has occurred with U.S. government entities. In January 2004, the U.S. Department of the Treasury planned to publish nearly 10,000 e-mail addresses on the Web, violating its privacy promise to consumers who used e-mail to comment on a government proceeding (McCullagh, 2004).

Purchasing prescription drugs from Canadian pharmacies online provides unique benefits to U.S. consumers who often shoulder a high cost burden. However, the legal and ethical issues of purchasing from the online market challenges what has historically occurred in the past with legislation and regulation. The following sections will address the issues of privacy and trust from its broader perspectives to the specific application of purchasing pharmaceuticals online from Canadian pharmacies.

Privacy Policies, Practices, and Preferences

Privacilla.org is a coalition of businesses and individuals encouraging a pro-technology and free-market economic view and endorses strong privacy rights on the Web (Privacilla.org, 2002). Privacilla.org (2003, p. 3), formulated a definition of privacy designed to "solidly capture the concept of privacy." The organization claims that failure to define the term within the context of the cause in which it is being used has resulted in failed policy initiatives. For the purpose of preventing the abuse and misuse of information provided by Internet consumers

> Privacy is a state of affairs individuals experience having to do with the amount of information about them that is known to others and on what terms. Specifically, privacy is the subjective condition that people experience when they have power to control information about themselves and when they have exercised that power consistent with their interests and values. (Privacilla.org, 2003, p. 30)

Privacilla.org's definition of privacy is intended to protect the privacy of consumers without restricting information sharing by marketers. Privacilla.org (2003) contends that the legal regulation of information sharing among corporate affiliates (which has been promulgated in California) has more negative than positive potential effects and does not correspond with the desires of most consumers. According to Privacilla.org (2003), "Perhaps the most important, but elusive, part of privacy protection is consumers' exercise of power over information about themselves consistent with their interests and values" (p. 4). In fact, California regulations are more consistent with the European Union's more stringent regulations on gathering, aggregating, and buying or selling consumer data (Reisch, 2003). California's Online Privacy Protect Act of 2003 became effective on July 1, 2004. It requires operators of commercial Web sites who collect information about California residents to post their privacy policy conspicuously on their Web site ("California Online," 2003). Cadogan (2002) predicts that the global nature of e-commerce will generate a trend in that direction.

Volokh (2000, p. 88) acknowledges that U.S. law currently places few restrictions on the communication of information by private parties. However, contract law can be used to enforce protection. He states, "If a business promises to keep information private, consumers can hold it to that promise." They can also threaten not to deal with businesses

that refuse to uphold privacy obligations--"a powerful threat in today's competitive marketplace" (p. 88). Arrison (2002) agrees that the primary control for Internet privacy lies in contracts, not regulators. Arrison argues that it is in the best interests of online businesses to respect the privacy concerns of consumers since they can simply switch to another retailer. She also contends that consumers are best served if they provide information that enables them to receive customized information and perks. Thus, Internet businesses have the obligation to respect consumers' privacy, thus leading to making consumers more comfortable in disclosing personal information to the mutual benefit of both parties. Essentially, legal regulations, self-regulation, and consumer preferences interact to maintain ethical privacy practices.

The research reviewed for this project supports the assertion of Privacilla.org (2003) that consumers' privacy preferences vary considerably. However, concerns with privacy are ubiquitous in the literature and are especially prominent when the topic is related to disclosing consumers' medical information.

Privacy and Trust

Culnan and Bies (2003) define *information privacy* as "the ability of individuals to control the terms under which their personal information is acquired and used" (p. 326). The authors maintained that consumers' perceptions of fairness play a key role in their willingness to disclose personal information. Alternatively, individuals are willing to disclose personal information for some social or economic benefit, as long as disclosing the information will not cause them harm. While there is a large body of research supporting this premise in the context of interpersonal relationships, Culnan and

Bies stress that it applies to consumer relationships, and can thus be applied to a variety of online and physical marketplaces.

Culnan and Bies (2003) note that the U.S. government currently takes a reactive mode with regard to consumer privacy issues. Congress typically takes action only after a specific problem has been identified and then reactively attempts to correct the issue only after each specific issue is identified. This is why there are separate laws and regulations governing medical records, financial records, credit reporting, information collected from children, and other similarly focused legislation. In most cases, legislation is enacted when businesses and consumers demand the government to act.

Culnan and Bies (2003) suggest that this conventional approach is inadequate in the face of consumer concerns over disclosing information online. They predict that persistent consumer concerns about privacy may ultimately lead the U.S. federal government to pass online privacy legislation for a number of reasons. First, consumers' apprehension about privacy threatens to hamper full utilization of online commerce. Second, alternatives to government legislation, such as self-regulation and technology, have not proven sufficiently effective. Government regulation is not the most cost-efficient solution, since it could raise the cost of doing business online. At the same time, "consumers incur significant costs in the absence of adequate privacy protection" (p. 333). To protect consumers, Culnan and Bies advise that, "To forestall government intervention, corporations need to regulate themselves in an enlightened manner" (p. 333). Ultimately, they predict that a synthesis of "self-regulation, technological solutions, legal solutions, and a vigilant media will be required over time to successfully protect

consumer privacy and address the range of preferences of American and global solutions" (p. 337) so consumers will see more benefit than cost in disclosing information online.

Consumer concerns about online privacy impede the full potential of the Internet and electronic business. The tremendous growth in e-commerce is illustrated by online retail sales in the U.S. soaring to $114 billion in 2003 (National Research Federation, 2004). Despite this growth, the figure falls short of the $380 billion projected by Forrester Research for 2003. Internet sales began to slow even before the 2001 economic stagnation and the dot-com bust; in fact, the slower than projected growth is often attributed to issues of consumer trust in online vendors. According to surveys of Internet users, two prominent concerns are perceptions that Internet businesses have poor, slow, or negligible customer service and customer apprehensions about disclosing personal information online. Resnick and Montania (2003) classify both these issues under the heading of "trust."

Consumer trust has been a focus of research across a wide variety of disciplines, and authors from a variety of areas have studied how human interactions affect trust. Hosmer (1995) states that trust involves an element of vulnerability. The person who places trust in another is vulnerable due to the lack of control over the actions of the other party. Based on published literature, Hosmer arrived at a definition of trust that is simple and applicable to a variety of economic exchanges, and advocates ethics. From this perspective

> *Trust* is the reliance by one person, group, or firm upon a voluntarily accepted duty on the part of the other person, group, or firm to recognize and protect the

> rights and interest of all others engaged in a joint endeavor or economic exchange. (Hosmer, 1995, p. 393)

Culnan and Bies (2003) emphasized that it is unrealistic to ensure trust as a complete reliance "upon a voluntarily accepted duty." However, evidence indicates that consumer trust is an important condition of both online and physical business commerce (Resnick & Montania, 2003). Consumers' perceptions of trust influence their desire to do business with a seller, and mutual trust between the two parties enhances the quality of economic interactions and results in more satisfaction between each party (Pennington et al., 2003). Trust has long been recognized as a key factor in customer loyalty, and perceived lack of trust (such as lacking a comprehensive stated privacy policy) can have negative repercussions on a firm.

Other definitions of trust indicate both its moral and ethical dimensions (Hosmer, 1995). Rose (2000) used the term "moral hazard" to describe the conditions under which Internet commerce takes place.

> Moral hazard means one party's actions are not observable by the other so the one in the dark must bear all the costs of protecting themselves but in doing so they will only receive some of the potential benefits of the transactions. (p. 23)

Consumers can protect themselves to some extent, but they have no control over the sale of their data to others. In addition, if they withhold information from Web sites, they lose the benefits of customization and various perquisites offered by different sites, and may not even be able to engage in online sales. However, consumers find ways to bypass marketers' required information by not giving accurate data. Forty percent of online consumers report sometimes providing fictitious data, so the marketer can find they have

inaccurate data. Culnan and Bies (2003) emphasize that optimal business relationships are characterized by trust on both sides.

Online commerce involves new technologies that enable storage and sharing of unprecedented amounts of information. Reisch (2003) states that making e-commerce safer and more secure involves a combination of legal, economic, and educational solutions in which all stakeholders must play an active part. The strategies Reisch recommends include government enforcement of new laws and regulations; consumer education; industry self-regulation and voluntary guidelines; third party verification systems, guarantees, and seals of approval; and the support of technological platforms.

Electronic Commerce and Trust

Pennington et al. (2003) proposes using system trust to define how consumers place their trust in online vendors. The authors define system trust as "a belief that the proper impersonal structures have been put into place enabling one party to anticipate successful transactions with another party" (p. 201). Pennington et al. (2003) views system trust from two perspectives. The first involves *structural assurances* or safeguards, such as regulations, laws, guarantees, and contracts that decrease consumers' perceived vulnerability and increase their trust in online firms. The second involves *situational normality*, "which makes the situation appear normal and reduces uncertainty in the transaction" (p. 201).

According to Resnick and Montania (2003), "Whereas trust develops over time, communicating trustworthiness must occur as soon as interaction with a site begins" (p. 212). Consumer research on face-to-face interactions, such as in traditional, non-electronic commerce, has found that competence, dependability, and likeability are key

factors in customers' trust (Pennington et al., 2003). In Internet transactions, the user interface and design of a Web page plays a role in defining the degree of consumer trust. According to Fogg et al. (2002), a Consumer WebWatch research report of 2,684 people evaluated the credibility of two Web sites to review 18 areas that people use when evaluating Web site credibility, and was one of the largest studies assessing how consumers evaluate Web sites. The study found that consumers often base their credibility decisions on the visual appeal of the Web sites as opposed to conducting unbiased evaluation strategies when assessing sites.

Online firms can use several methods to enhance trustworthiness of their sites. One method that increases consumers' level of trust is the use of privacy seals. Seals guaranteeing privacy and security may be supplemented by a rating system or "star" system denoting how well the site performs according to a set of criteria that offers evidence of vendor performance as perceived by users. Another way is the presence of a vendor statement that includes information about privacy and security as well as specific information for the type of transactions being conducted. However, Pennington et al. (2003) note that these statements do not necessarily include verification by third parties.

Pennington et al. (2003) explored consumer perceptions of trust in an experimental survey of 266 Internet users (170 women and 92 men with an average age of 42 years). Most reported going online daily, making purchases online, and frequently surfing the Web to find product information. The participants were told to browse a specially designed Web site as an online shopper in search of a DVD. They were instructed to click on any symbols offering additional information about the site. Upon completing the task, the participants were asked to fill out a questionnaire about their

experience with the site and submit it in order to be eligible to win a prize. They were also requested to fill out a page of personal information that would allow them to be contacted if they won (personal information was carefully separated from subject responses to maintain research anonymity).

Based on their results, Pennington et al. (2003) concluded that system trust is "a 'controllable' construct that can be used to directly influence perceived trust" (p. 213). Sites can use a variety of measures designed to promote trust and to influence consumers' positive perceptions of the Web site. Pennington et al. (2003) found that the site's reputation, often based on the firm's past performance, was found to be an important predictor of trust. The use of self-reported guarantees, such as money-back guarantees and assurances of security or privacy positively influenced consumers' trust and created a positive image regarding the site. Interestingly, vendor guarantees, which have no third party verification, proved more predictive of system trust than third party seals (pp. 213-214). Pennington et al. (2003) proposed that third party seals are probably more closely linked to issues related to actual purchases, which were not part of the study. The study offered a valuable framework for exploring trust in the area of online business and commerce (pp. 213-214).

Resnick and Montania (2003) explored using online trust with *semiotics*, "the study of signs and symbols that convey semantic and syntactic content and their use as a communicative tool" (p. 212). In the retail environment, "trust is the belief or expectation that the word or promise by the merchant can be relied on and the seller will not take advantage of the customer's vulnerability" (p. 213). In the arena of online commerce, trust is vital for the success of a firm

> A customer at an online commerce site lacks concrete cues to comfortably assess the trustworthiness of the site and therefore must rely on new kinds of cues. The interpretation of these cues drives the development of customer expectations of the trustworthiness of the vendor. (Resnick & Montania, 2003, p. 213)

Resnick and Montania (2003) maintain that the impact of Web site design rests on consumers' perceptions of three factors that influence decisions to purchase: customer service, reputation management, and privacy. The researchers created Web pages for fictitious Internet retailers selling flowers and related gifts. They varied the sites superficially to ensure they appeared as four distinct retailers while keeping basic information, such as prices, the same. Three important areas distinguished one firm from another: the presence and prominence of customer service links, customer ratings, and a privacy policy. After a pilot test, Resnick and Montania conducted their study on a sample of 64 adults ranging in age from 18 to 53 years. Most were frequent Internet users (83%) and 78% had purchased items online. The participants were told they were testing the usability of new Web sites.

Resnick and Montania (2003) found that each of the three "trust-focused" design elements had a significant impact on the participants' preferences for the Web sites and on their expectations of customer service, privacy protection, and merchandise quality. The authors state, "The presence or prominence of all three design parameters were positively associated with users' perceptions of each site and from this site they chose to make their purchase" (p. 230). They found neither the customer service links nor the privacy policy links offered explicit information on how much customer service would be provided or how the Web site protected consumers' privacy and personal data. However,

these links did enhance consumer perceptions that the sites did a good job with privacy, thus enhancing trust (p. 230). An interesting point was that a prominent display of product ratings also increased the subjects' perceptions of privacy protection. This result was not what the researchers had anticipated. They hypothesized that, "This effect may be due to a perception that other customers were happy with the company's performance in general and this generalized to include privacy protection perceptions" (pp. 230-231).

Pennington et al. (2003) and Resnick and Montania (2003) used concepts derived from marketing research and applied them to online commerce. Mears, MacNeil, and DeJarnette (2003) contend that the e-commerce explosion acts as a driving force in "reshaping the very nature of trust" (p. 1). These "new business drivers" include:

- *Blurred borders:* as more companies diversify and expand, "the lines defining where they begin and end become less apparent, legally, physically, and culturally" (p. 1).
- *Virtual marketplace:* the environment where consumers and vendors interact is created by a Web site's ability to elicit and "intelligently" use consumers' personal information.
- *Data aggregation:* as the tools for collecting, aggregating, and disseminating data proliferate, both individuals and companies are concerned about privacy risks.

The concepts of consumer privacy and trust originated long before the advent of online commerce. However, the nature of electronic commerce requires new mechanisms and legislation to protect the privacy of consumers' personal information. For online

commerce to reach its potential will require addressing consumer concerns and building trust to a degree at least equal to that involved in face-to-face interactions.

Privacy Policies

The protection of privacy in the U.S is a mixture of laws, court decisions, and self-regulation (Larson, Larson, & Greenlee, 2003, p. 50). Other sources point out that in the U.S., "a consumer's privacy is protected primarily by the goodwill of businesses" (p. 50). While this practice may have sufficed in the realm of traditional commerce, few consumers are willing to disclose personal information online based on faith in the vendor's "goodwill." American business sources tend to express a preference for contracts over regulation as the major method for controlling information flow and commercial interactions (Arrison, 2002). Different types of transactions fall under the jurisdiction of different agencies. Online pharmaceutical companies generally fall under the jurisdiction of the FDA, which controls the importation and safety of the drugs, and the FTC, which enforces consumer protection laws (Sweet, 2001).

Rothstein (2001) found both differences and similarities between the privacy protection provided by U.S. and Canadian legislation. The similarities outweigh the differences since both countries have laws at both the federal and state or provincial levels. However, the Canadian regulations are more comprehensive than U.S. laws, which lack uniformity, and differ among the various states.

Kobsa (2002) specifies that, "Privacy laws protect the data of identified or *identifiable* individuals" (pp. 65-66). Privacy laws have been enacted by more than 30 countries as well as by U.S. states and Canadian provinces. Kobsa contends that while privacy laws have numerous superficial differences, they are generally founded on a

small number of privacy principles. These principles are derived from recommended privacy guidelines adopted by the Organization for Economic Cooperation and Development (OECD) in 1980. The OECD privacy principles include: (a) Collection Limitation Principle, (b) Data Quantity Principle, (c) Purpose Specification Principle, (d) Use Limitation Principle, (e) Security Safeguards Principle, (f) Openness Principle, (g) Individual Participation Principle, and (h) Accountability Principle.

Kobsa (2002) advocates the enactment of an international treaty on information privacy. Whether that is feasible in the near future, the virtually universal concern for online privacy will encourage businesses and government to coordinate self-regulation and legislation to alleviate privacy concerns and conflicts.

Canadian and U.S. Health and Medical Information

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has provisions called “administrative simplification,” designed to promote development of a uniform, technology-based health information system (Choy et al., 2001). Part of HIPAA regulations is the “Privacy Rule,” which became effective as of February 26, 2001. It is a set of basic national privacy standards and fair information practices that protect Americans' personally identifiable health information (Rothstein, 2001). With the understanding that privacy is of utmost importance, Congress included a requirement that if it did not enact health privacy legislation by legislative deadline, the Department of Health and Human Services would be required to do so. However, the authority of the Department only extended to three health care entities: health care providers, health plans, and health care clearinghouses. This limitation excludes many health-related Web sites. Thus, depending on the owner or operator of a given Web site, a site offering health

or medical services, including prescription drug sales, may not be covered by HIPAA rules. Choy et al. (2001) and Rothstein (2001) concur in stating that part of the HIPAA regulations specifies which "covered entities" fall under these auspices, and these may not include some types of Internet based pharmacies

Canadians are protected by two pieces of legislation: the Privacy Act and the Personal Information Protection and Electronic Documents (PIPED) Act. The Privacy Act (1983) protects Canadian citizens by placing controls on the collection and use of private information. The PIPED Act (2001) regulates how private industry is able to collect and use personal information about its customers (Canada Privacy Commissioner, 2002).

The Privacy Commissioner of Canada has stated that, "Personal health information—information about the state of our bodies and minds—is arguably the most private information of all. When that information is not treated with the utmost care and confidentiality, the consequences can be disastrous" (Canada Privacy Commissioner, 2003a, p. 24). PIPEDA covers health information broadly, as it applies to all personal data collected, used, or disclosed in the course of commercial transactions (McCutcheon, 2002). The basic principle of PIPEDA is that individuals have the right to consent to having personal data collected, used, or distributed. Additionally, PIPEDA outlines 10 principles of fairness with which organizations are expected to comply. The expectations for privacy, both explicit and implicit, in PIPEDA far surpass the perfunctory legal efforts to guard information privacy in the U.S.

Beginning January 1, 2004, pharmacists in Canada were required to comply with PIPEDA. Patients, including those utilizing online sites, must be informed of what

information is being collected, how the information will be used, and with whom the information will be shared (Canadian Pharmacists Association, 2004).

Rothstein (2001) used the term "patchwork" to describe the industry-specific U.S. laws that operate within a system of self-regulation. This includes the recent enactment of a "detailed medical privacy law" that "covers actions of both public and private actors" (p. 345). Rothstein predicts that the growth of online pharmacies will lead to greater consistencies in the regulation of health information between Canada and the U.S. However, American businesses across sectors are reluctant to give up the self-regulation that appears to have served the economy well for so long.

Rothstein (2001) divides online pharmacies into three categories: (a) pharmacies that offer a limited number of select drugs, (b) pharmacies created from brick-and-mortar pharmacies, and (c) "full service virtual pharmacies" such as drugstore.com (p. 53). Many pharmaceutical firms also have online presences to provide consumer and professional information. The Eli Lilly case illustrates how these sites can jeopardize personal information as a consequence of lax privacy procedures (Beales, 2002).

In the Eli Lilly case, the breach of privacy was unintentional and due to failure to adhere to privacy protection protocols (Beales, 2002). Surveys of health professionals with access to sensitive medical information have reported that they recognize inherent threats to consumer privacy and support measures designed to minimize them (Baumer, Earp, & Payton, 2000). The recommendations of health professionals largely correspond with administrative proposals.

Pharmacies based in the U.S. are subject to both federal and state regulations (Rothstein, 2001, p. 358). Federal laws primarily cover the handling of personally

identifiable health information by federal agencies and their private subcontractors. State laws present the most powerful mechanism for controlling consumer health information and records, although the laws vary considerably by state and address different concerns, often related to the era in which they were enacted. However, Rothstein (2001) emphasizes "providing health services over the Internet is a multi-jurisdictional activity that could, in theory, implicate the law of all 50 states" (p. 358).

In addition to protection under PIPEDA, the Health Information Privacy Code provides the Canadian health care industry with an industry-specific self-regulatory mechanism for protecting the privacy of personal health data (Rothstein, 2001). PIPEDA was enacted to address gaps in protection resulting from the government-sponsored single-payer of health care. Under these laws, Canadians are better protected from the misuse of health and medical information than their American counterparts. In January 2004, the Canadian Pharmacists Association issued a statement detailing the privacy laws under PIPEDA and the Health Information Privacy Code, as well as addressing the provincial legislation governing privacy protection (Canadian Pharmacists Association, 2004).

Pharmacy regulation

The difference in privacy laws between the U.S. and Canada can raise a significant issue among the posted policies for Canadian online pharmacies. Although these sites originate in Canada and are bound by Canadian laws, they affect American consumers. Canada has more stringent legal protection for its businesses than those that operate in the U.S. and are covered by a myriad of provincial and federal regulations.

American privacy and online pharmacy Internet protection falls under a multitude of agencies and regulations. According to Sweet (2001), online pharmaceutical firms are under the primary jurisdiction of two agencies, the FDA and the FTC. The FDA controls the importation and safety of the drugs. The FTC enforces consumer protection laws, such as privacy policy postings on Internet sites. According to Rothstein (2001), U.S. privacy protection dealing with medical records contained on American Internet sites could fall under HIPAA legislation. One portion of HIPAA regulations is the "Privacy Rule," which became effective February 26, 2001. This rule outlines privacy standards and fair information practices that protect Americans' personally identifiable health information.

Another legal issue that affects the online pharmacy arena is the 1994 North American Free Trade Agreement (NAFTA). This Agreement eases border restrictions between the U.S., Mexico, and Canada. However, Graham (2003) states that the cross-border pharmaceutical trade violates the principles of free trade and possibly NAFTA. He indicates that due to the cross-border trade in pharmaceuticals, the Canadian government is not giving foreign-owned manufacturers "fair and equitable treatment and full protection and security," (p. 17) one of the articles of NAFTA.

Both Canadian and U.S. pharmacies are regulated at both the federal and state or provincial levels (Rothstein, 2001). In addition, pharmacies in both countries must obtain licensure in the state or province where they are based. In 40 states, legislation requires that out-of-state pharmacies or non-resident pharmacies selling prescription drugs comply with a specified set of regulations that range from providing evidence of licensure to maintaining a toll-free telephone line (displayed on each prescription drug label) that

enables customers in the state to communicate with the pharmacy (U.S. General Accounting Office, 2000). Since 1998, several states have enacted legislation to regulate Internet pharmacies: Indiana, New York, Illinois, California, New Hampshire, Arkansas, Nevada, and Texas (Gordon, 2004). The states vary in their specific laws but, in general, all require that online pharmacies comply with state regulations and licensing laws and maintain a specifically designated governing body.

State and federal legislatures may propose laws to protect consumers who utilize online pharmacies, but not all proposals are enacted. For example, one of the initiatives proposed by the Clinton Administration in 1999 was to protect consumers from the illegal sale of prescription drugs via online Internet sites. Part of the proposal was a new Federal requirement to enable consumers to identify legitimate Internet pharmacy sites, as well as strengthening FDA authority to investigate the sites (U.S. White House, 1999).

The U.S. General Accounting Office (2000) and FDA official Hubbard (2003) emphasize that they recognize the potential benefits of online prescription drug purchasing for American consumers. Hubbard cites several factors that consumers find positive, especially those individual who are disabled or ill. These benefits include ease of use, convenience, privacy for consumers who have problems they do not wish to discuss in person, and vastly expanded information access. He also proposed that technology could reduce medication errors, thereby making prescription drug purchases safer. The FDA's main concern is the safety of prescription drug sales by pharmacies outside U.S. jurisdiction.

The FDA has traditionally exempted the importation of drugs from Canada from federal restrictions under the "personal use" guideline. This action makes it legal for

Americans to bring in small quantities of prescription drugs (no more than a three-month supply) for personal consumption (Parloff, 2004). Recognition of this guideline inspired enterprising pharmacists in Manitoba and Winnipeg to establish the first online pharmacies targeting U.S. consumers, RxNorth.com and CanadaMeds.com, respectively. Within a short time, the pharmacy sites were thriving businesses that generated a proliferation of online pharmacies and a tremendous amount of publicity, both good and bad.

The dominant reason for American consumers' interest in Canadian pharmacies is the cost of prescription drugs in the U.S. compared to the relatively lower prices in Canada. There are several reasons for the higher prices in the U.S. One is the overall expense of health care in the U.S. compared to other countries, and the second is the amount of money U.S. pharmaceutical firms invest in research and development (R&D) (Cohen, 2004; Graham, 2003). The paradoxical effect of the investment in R&D is that prescription drugs imported from Canada are frequently *re-imported.* That is, despite alleged concern over the manufacture of drugs outside the U.S., many were manufactured in the U.S. Because of the high cost of R&D, pharmaceutical firms pass the costs on to consumers.

There is a third reason, however, for the large difference in cost between the two countries, pharmaceutical price controls imposed by the Canadian government. Statements by U.S. officials indicate that these controls present problems for U.S. consumers. In November 2004, FDA Chairman Mark McClellan attacked Canada's price controls and stated they encourage illegal activity, contribute to unsafe cross-border safety risks for unapproved drugs, and reduce funding for drug research (Webster, 2003).

However, a Canadian health analyst suggested that the attack was a “smoke and mirrors game” and suggested that the FDA’s remarks were inappropriate (Webster, 2003). The FDA has strengthened its opposition to the businesses engaged in this online commerce. Thompson (2004) stated that in November 2003, the FDA took legal action against a U.S.-based online pharmacy, Rx Depot, and a federal judge sided with the courts to shut down the firm. Thompson further explained that since the FDA faced significant legal challenges in bringing charges against Canadian-based pharmacies, the FDA may take legal action against states and cities that are encouraging this practice. In addition, in 2000, the FTC settled charges with a group of online pharmacies that indicated they operated medical and pharmaceutical facilities they did not have or did not adhere to their stated privacy policies (U.S. Federal Trade Commission, 2000b).

Although the FDA has taken action against online business, they have been less likely to act against individuals. Whitwham (2003a, p. 759) references Jeff Poston, executive director of the Canadian Pharmacist Association, saying that the FDA does not interfere with consumers engaged in cross-border commerce because many of them are senior citizens without insurance. He claims that if the FDA proceeded to prosecute these seniors, they would have a difficult moral position to defend. The FDA would also face the political wrath of seniors and other consumers who purchase Canadian drugs.

U.S. consumers’ increased use of Canadian mail-order pharmacies has led to repercussions for Canadian consumers and pharmacists. The pharmaceutical companies have considerable influence and have used this power in an effort to limit the growth of the online Canadian pharmacy industry. Since January 2003, several major international pharmaceutical firms, including GlaxoSmithKline, Pfizer, AstraZenica, and Wyeth have

made individual efforts to halt the importation of drugs from Canada into the U.S. (Cohen, 2004; Korcok, 2004; Parloff, 2004). In January 2003, GlaxoSmithKline, the world's second largest pharmaceutical manufacturer, sent letters to Canadian Internet pharmacies announcing they would stop supplying products to pharmacies that sold drugs to U.S. consumers (Gregoire, 2003). Those pharmacies that also sold products to Canadian as well as U.S. consumers could find they can no longer service either group, thus leaving Canadian citizens with fewer pharmacy choices. Vivian (2003) states that in early 2003, the U.S. FDA issued a policy letter against businesses that re-import prescription drugs from Canada. The FDA also warned Congress that mail-order pharmacies are breaking current U.S. law could face stiff criminal penalties, and warned that re-importation could result in counterfeit drugs reaching U.S. patients.

Canadian officials in business and government have expressed concerns that the flow of drugs into the much larger American consumer market will result in a shortage of prescription drugs in Canada. Several Canadian medical organizations, such as the College of Physicians and Surgeons of Alberta and the Canadian Medical Protective Association (CMPA), advised members against co-signing American prescriptions, under threat of disciplinary action (Gregoire, 2003). The Association provides an example that if an American consumer files a lawsuit against a Canadian pharmacist, the Association could not defend the member against U.S. litigation. Canadian consumers also face ramifications due to the growth of these pharmacies.

This cross-border market is viewed with trepidation by some Canadian researchers and legislators. Canada NewsWire quotes a research analysis conducted by Pangea Consultants (a health care industry specialist firm), which indicates American health care

needs are so vast that Canada would be unable to meet the U.S. demand, and that attempting to meet U.S. needs would adversely affect Canada's health care system. The research states that an increase in cross-border sales could have the following adverse affects on Canada: (a) retail drug shortages among Canadian pharmacies, (b) drug price inflation in Canada, (c) pharmacist shortage because of diversion to U.S. patient care ("New mood," 2004). Statistics by IMS Health Canada show a large increase in cross-border online sales from 2002 to 2003 among the various Canadian provinces, and states that Manitoba ships 45.5% of its total top 10 drug classes to the U.S. The agency raised the concern that because these drugs are the ones most sought by both countries, Canadian patients could be placed in direct competition with U.S. consumers for these drugs ("Manitoba still tops," 2004).

In the most recent round of the dispute, Canadian Health Minister Ujjal Dosanjh stated that, "The practice by some doctors of counter-signing prescriptions without actually having a relationship with the patient and properly assessing the patient is absolutely unethical and unprofessional" (Krauss, 2004, p. A1). Even more emphatically, Dosanjh declared, "Canada cannot be the drugstore of the United States" (p. A1).

Besides Canadian industry groups' apprehension, members of the Canadian government have also expressed concern about the rise of mail-order pharmacies and the impact on Canadian consumers. In November 2003, Senator Robertson of the Canadian Senate (C-NB) reviewed Internet pharmacy risks posed by Canadian pharmacy and medical associations about the safety impact of this border, and concerns about the drug supply for Canadian consumers (Canada Parliament, Senate, 2003).

Although some Canadian lawmakers and healthcare associations have expressed unease with the growth of Canadian online pharmacy sales to U.S. consumers, other Canadian authorities have encouraged this practice after recognizing growth and profit potential. Whitwham (2003b) stated that in 2003, "Manitoba began issuing licenses to online pharmacies, authorizing them to sell to international customers" (p. 1033). He also quoted Ron Guse, registrar for Manitoba's pharmacists, who claims certain pharmacies are writing prescriptions for U.S. customers without reviewing the medical background of the patient.

Online Canadian pharmacists claim that they will ultimately prevail over their opponents. Krauss (2004) noted that online Canadian pharmacies sales are still increasing albeit at a much slower pace. In addition, some of the biggest companies are making radical changes in their business plans. Ironically, some of the plans include moving the pharmacies to locales outside of either Canadian or U.S. jurisdiction, a move that could expose consumers to far greater risks than the purchase of re-imported, U.S.-manufactured drugs.

With an increase in the number of uninsured U.S. citizens and rising health-care and pharmaceutical costs, consumers are concerned about the availability of affordable drugs. Korcok (2002) indicates politicians have promised consumers greater privacy regulations, access to cheaper drugs from Canada, and the right to sue HMOs, although none of these has been fulfilled. Because of consumer frustration, many constituents are turning to voting for receptive congressional representatives as a way to contain medical costs and to ensure that the FDA does not enforce laws preventing them from importing drugs from Canada. Korcok (2002) quotes a study of the American Association of

Retired Persons (AARP) showing that 26% of retirees would vote against any senator who prevents passage of legislation mandating a prescription drug benefit. A 2003 ABC News-*Washington Post* poll indicated that 70% of U.S. respondents believed that it should be legal for consumers to buy prescription drugs outside the U.S. One in eight respondents said they or someone in their household had done so ("Poll: Public supports," 2003).

In a survey conducted in October 2003, 77% of Americans deemed it "unreasonable" for pharmaceutical companies to prevent Canadian pharmacies from selling prescription drugs to Americans online (Cohen, 2004). An estimated 35% of Medicare recipients lack prescription drug benefits and some 22% of seniors are unable to fulfill prescriptions due to the high cost or skip doses to make a prescription last longer. In view of these circumstances, Cohen notes that, "even breaching the law can appear justifiable" (p. 16).

One can argue that virtually all the laws governing Internet privacy and commerce are in a state of flux. Existing laws are inadequate for addressing the challenges of conducting business on the Internet. As more consumers utilize online firms for purchases of all types, they still express numerous concerns related to the protection of personal information on the Web.

Privacy Practices and Consumer Behavior: Empirical Research

Internet Privacy Practices

Leizerov (2001) conducted a comprehensive investigation of the consumer privacy practices of 145 Web sites randomly selected to represent several industries and categories. These included: (a) Web sites offering computers and Internet products and

services, (b) Web sites providing news information, (c) Web sites providing travel information and services, (d) Web sites providing health information and related products, (e) Retail sites selling consumer products that did not fall into any other category, (f) Entertainment and sports, including videogames and sports, and (g) Portals, including sites such as Yahoo! that provide online information only, a search engine, personalized services, and e-mail service. The Web sites were examined according to their compliance with and attitudes toward privacy regulations, intrusiveness of data collection, integrity through ethical privacy practices, and transparency and accountability.

Leizarov (2001) found that economics had a significant impact on Internet privacy practices. Online firms whose existence depended on a strong commercial relationship with Internet users showed the most responsible privacy practices. Alternatively, portals are primarily dependent on advertisers and marketing partners for their success (and thus stand to benefit from collecting more data about customers' interests, preferences, and demographics). Moreover, they are usually further removed from the consumers and also had the most lax attitude about privacy protection.

The online firms' understanding of the need for policies that respect consumers' privacy preferences is an extension of the trust that is essential to all business, regardless of whether they are online or on-ground (Hosmer, 1995). Online businesses that also run brick-and-mortar operations showed significantly more respect for trust building practices than those whose presence was exclusively online. However, Leizerov (2001) proposed this might be due to most of the e-businesses being young companies at the time, as Internet technology is relatively new. Online businesses such as Amazon.com

have had time to develop more expertise in establishing positive consumer relationships. Leizerov also found that Web sites in the "Computers and Internet" category also had high scores on compliance with privacy rules and trust building practices, second only to traditional retailers with an online presence. This applied not only to companies selling expensive items but also to Web sites that offered product reviews and free software downloads. Leizerov suggested the practices reflected recognition that their sites attracted savvy Internet users with knowledge of how to protect their privacy online.

Privacy Seals

Privacy usage seals are available to Web sites through programs where "trusted" organizations certify that Web sites meet strict privacy usage for the information collected from their customers. The seals represent visible efforts by online organizations to demonstrate that they protect consumer privacy through self-regulation (Bahadur, Chan, & Weber, 2002). BBBOnLine and TRUSTe are probably the best known of the privacy seal organizations. TRUSTe has two major seal program options relevant to online pharmacy businesses: the Privacy Seal Program and the E-Health Seal Program (TRUSTe, 2004). The Better Business Bureau runs another popular seal program, BBB. They have two programs that e-commerce sites can use to address consumer privacy concerns, the reliability seal program and the privacy seal program. The reliability program requires businesses to abide by BBBOnLine's Code of Online Business Practices and Code of Advertising. Its privacy seal program requires firms to have stated online privacy pages, which conform to BBBOnLine's privacy guidelines (BBBOnLine, 2004).

Consumer marketing research indicates that the prominent display of a privacy seal has a significant impact on consumers' perceptions of trustworthiness (Pennington et al., 2003). However, there is an important question of whether TRUSTe, BBBOnLine, WebTrust, or other privacy seal programs have the power to enforce their stated privacy protection principles (Moores & Dhillon, 2003). Once again, the seals raise the issue of how to achieve a balance between industry self-regulation and government regulation while protecting the interests of consumers and vendors.

Leizerov (2001) also reported substantial differences in the practices of Web operators who were members of BBBOnLine and TRUSTe. Namely, "TRUSTe, which depends economically on the fees paid by its members was found to be significantly less rigorous in monitoring them when compared to BBBOnLine" (pp. 230-231). He observed that on some measures, Web sites that were not part of any seal program fared better than members of TRUSTe. Economic factors proved to be the overriding predictor of privacy and trust building practices, as evidenced by both the high scores of the online retailers and the lower monitoring efforts of the fee-based TRUSTe.

Although seal programs could alleviate some consumer privacy concerns, the literature indicates that they are not without controversy. Larson et al. (2003) states that although firms have set up seal programs to address consumers' privacy trepidation, these programs are self-regulated and depend on member self-compliance. Larson notes that another problem is that consumers could become confused because each program treats Web sites in a slightly different manner. Moores and Dhillon (2003) validated Larson's research. Their study analyzed three privacy seal programs: TRUSTe, WebTrust, and BBBOnLine by reviewing the posted features of each of the sites including what

information is collected, how the information is collected, opt-in options, complaint procedures, feedback from the online community, the number of recipients in each program, the review process, and the fees to use the program. The results indicated that all three organizations have similar principles on data collection, feedback, and security. However, procedures are different for each firm, and could be a factor for consumers to consider when placing their trust in a program.

Even when Web sites contain these third-party approval seals, consumers may be ambivalent towards placing great faith in them. Brown (2002) cites a Pew Internet & American Life study, which indicates few people bother to determine if a site's privacy policy has been independently checked by a third party, such as a privacy seal program.

Fair Information Practices

When online firms include a privacy page on their Web site, the overall policy can contain a variety of selections. While there can be numerous policy segments, the overall policy should adhere to general practices. The U.S. Federal Trade Commission (2000) issued a Fair Information Practices report to Congress in May 2000. The Commission recommended that commercial Web sites that collect personal information comply with four Fair Information Practices: (a) notice, where Web sites should provide consumers with understandable notice of their privacy and information practices, including what information they collect; (b) choice, where Web sites should offer customers options on how their information will be used, as well as how that information is disclosed; (c) access, where Web sites should allow consumers access to their data as well as opportunities to correct inaccurate information; and (d) security, where Web sites should

take reasonable steps to protect personal consumer information (U.S. Federal Trade Commission, 2000).

While these four practices are stated in general terms, the specific policies and practices for each site depend on the technical and business procedures of the firm. Numerous explicit policies incorporate the functionality of the four fair information practices. However, even with inclusion of fair practice principles, consumers may find privacy policies too complicated to understand. FTC Commissioner Sheila Anthony believes online privacy policies are too difficult for consumers to locate and contain too much complex legal jargon for the average person to understand. She believes "companies need to standardize their policies in much the same way that food companies use nutrition labels that make it easy for consumers to count calories" (Thibodeau, 2001).

Cadogan (2001) conducted a case study of the incorporation of Fair Information Practice Principles in the privacy policies of three well-known Internet and distinct Internet entities: Amazon.com, Dell, and the Privacy Alliance. Amazon and Dell both store cookies that enable them to maintain a profile of their customers. Cookies are small text files placed on a user's computer by a site that wishes to collect information or to assist the user in site navigation. Using cookies allows online firms to individualize their marketing techniques (Amazon's customer recommendations are a notable example), a convenience to both marketer and consumer. Both Amazon and Dell also offer customers the option of receiving emails to inform them of updates, complementary products, and sometimes, special offers to previous buyers. Cadogan noted that the predominate preference of online merchants is the opt-out strategy (asking to be removed from notification lists) versus opt in (having to request to be on a notification list).

Direct and Indirect Data Collection Methods

Online customer information can be accumulated two ways, directly and indirectly. Data can be collected directly from consumers who enter their information via forms or email on the business's Web site. Indirect collection is a method used to gather data through a secondary source. Normally, consumers enter their personal information on a variety of sites. Indirect collection software systems were created to alleviate the burden of remembering a variety of personal data to log into each site. Microsoft's Passport profile is an example of indirect collection. A consumer's personal information, such as password and credit card number, is stored in a centralized database. Then, instead of signing onto various sites, the consumer merely references the centralized profile in order to access any Web site they normally use. Although methods, such as Microsoft's Passport, can reduce the number of times consumers enter personal data, they are not without problems. Regan (2003) states that in 2003 a serious flaw was discovered in the software that could have compromised consumers' privacy data. In 2002, the FTC found that Microsoft was making false claims for privacy and security with this software (U.S. Federal Trade Commission, 2002c). With security issues related to Microsoft's products a concern within the Internet community, consumers may believe that their personal information is better protected when collected through direct means.

Medical Data

In order to fulfill prescriptions, licensed online pharmacies may require their customers to divulge medical history. The online firms may also provide advice on the prescription order, as well guidance on medical issues. Although consumers need timely and accurate access to drug information if they use these sites, accurate data is not

necessarily provided. A 2001 study of 104 e-Pharmacy Web sites by Bessell, Anderson, Silagy, Samsom, and Hiller (2003) found that consumers who self-select medicines from online sites have insufficient access to information when ordering their prescriptions, as well as limited information about how to use the products safely and appropriately. This was one of the first studies that evaluated the quality of information published on online pharmacy Web sites and indicated that sites often provided low-quality information both on the sites and well as insufficient information in the packaging. One of the underlying factors relating to potentially harmful effects of using the products was inadequate exchange of information between the site and patients. The authors stated that the medical history and personal information the sites collected, such as current medications the consumer was taking, was often insufficient to safeguard against adverse drug interactions.

Cookie Usage and Web Bugs

Cookies have benefits to both online firms and their users. Sites can use information for marketing purposes, such as surfing habits. Consumers use them for faster site navigation, such as when login information is saved for quicker logins. However, consumers fear too much personal information can end up in a firm's database from such protocols, especially when they never gave explicit consent for firms to gather this data.

When privacy standards for cookies were being created, the FTC and several subgroups of the Internet Engineering Task Force (IETF) standardization committee disagreed over the privacy principles to be included in cookie standards (Kristol, 2001). Although Kristol claims that better privacy features could have been applied to the

original cookie project, such recommendations could be applied to new standards projects to offer better privacy protection for consumers when using cookies. He recommends future projects address concerns related to the full range of cookie users such as browser representatives and Web site marketers and operators. New standards efforts cannot be the sole means to solve cookie issues, voluntary self-regulation programs may also need to be implemented.

Olsen (2000) mentions that cookies can also be combined with Web bugs (clear gifs) to identify personal information such as a phone number and address, as well as to monitor surfing habits without a person's knowledge. He indicates these bugs serve as electronic tags and send information back to a marketer's server, thus keeping personal tracking information about an individual's surfing habits. Not only could this combined technology be used to gather demographic information, it is conceivable that personal medical information could be gathered, along with a consumer's surfing habits of the online pharmacy and related medical information sites. Although there are concerns with private industry collecting information from cookies, the practice transcends this arena, and extends to government sites. A study by Bahadur et al. (2002) reviewed U.S. government problems with controlling cookies and Web bugs on government sites. Although the government has prohibited cookies from their sites since 2000, the audit found that 23 government sites had 300 cookies on various pages and 23 Department of Commerce pages had Web bugs (Bahadur et al., 2002). Clearly, although laws may exist to protect consumers, they are not always observed.

Because there are benefits to cookies, Leizerov (2001) does not recommend that users turn off the ability to accept all cookies. Instead, he states that enhanced privacy

may be augmented by setting attributes on their Internet browsers to reject cookies that do not bear the name of the domain they visit.

Profiling Information

Web developers use cookies to collect a variety of marketing and other information stored on a person's computer. This information can be used for personal profiling and data mining. This profiling information can include Internet Protocol (IP) address, browser types, referring Web site address, log files, usage tracking, and domain name. Cadogan (2002) states that online firms can use this data to track consumers' online movements and actions, and businesses can use this information to create targeted advertisements.

Information Update Policy

Consumers possess two primary methods to control personal information from being divulged to online sites. First, they may have the ability to request that the online business updates incorrect information. Second, they may be able to request that their data be deleted from the information database. A study of 21 health-related sites by California HealthCare Foundation found that only 10 sites allowed users to correct information collected voluntarily (Goldman, Hudson, & Smith, 2000).

Under HIPAA, medical Web sites defined as "covered entities" are required to comply with the privacy regulations. These regulations provide consumers with the right to see, copy, and correct their health information at online sites, and the firms are required to respond to users' requests by a specific deadline (Choy et al., 2001). Although online pharmacy consumers who wish to update their online data may assume they are

covered under HIPAA, this may not necessarily be the case. Online pharmacies are not specifically defined as "covered entities" under HIPAA. Although consumers may value the ability to view and update their information in a positive light, this protection may not be mandated for some online pharmacy sites. The ability to update consumer information is not legally mandated across all types of online business sites.

Disclosure to Third-Parties

Not only do primary sites collect personal data about the consumer, but it is also possible that those firms share this information with third-party firms or affiliates. In order to observe principles concerning informed notice of the Fair Information Practices ideals, it is important for consumers to understand where their information is being disseminated. A study by the California HealthCare Foundation of 11 online medical sites with third-party networks showed that only five of these sites stated that third-party networks were able to collect information about users (Goldman et al., 2000). This may lead to the consequence of a firm sharing data with an affiliate firm unknown to the consumer.

Online firms may use a wide variety of idioms to describe their relationship with third-party firms, and may include various "relationship" terms in their privacy policies. These various terms may confuse consumers who may question the strength of the relationship and data sharing among the firms. For example, the term "affiliate" could be interpreted broadly to mean any type of general partnership between two firms. The use of general terminology relating to disclosure by third parties is common. Goldman et al., (2000) found that although the Web sites in their study were likely to notify users about information disclosure, they included broad statements about such disclosures.

Security

Online firms often face a dilemma when posting detailed security elements on their privacy sites. If they do not post information on the methods they use to secure customer data, consumers may conclude that the firm does not practice safe computing and information security practices. However, if they post security policies, in detail, hackers may use this information as a starting point to gain unauthorized access to the system. Therefore, firms may maintain a balance of documenting the security of their systems. They often provide a policy to reassure consumers that security is taken seriously, but not supply details sufficient to provide ammunition for hackers to bypass security controls. The Online Privacy Alliance, a self-regulatory group promoting privacy policies for private sector Web sites, provides general guidelines for firms to follow when dealing with privacy issues: (a) sites should take appropriate measures to ensure the reliability of consumers' information and take precautions to safeguard it, (b) sites should take reasonable steps to ensure that affiliates and third parties who share this data are aware of their security practices and these associated firms also engage in safe security practices (Privacyalliance.org, 2003a).

Although there is concern among consumers as to the safety of their data being held in corporate databases, it is to the advantage of firms to ensure the data is secure. According to Cadogan (2002), firms have invested so much time and money to develop systems and collect personal and marketing information on Internet users, it is imperative they develop safe and secure systems to prevent hackers and other unauthorized people

from stealing the data. Data has value, and it is in the best interest of firms to develop adequate security and data control mechanisms.

COPPA Law

The Children's Online Privacy Protection Act (COPPA), enacted in 1998, is intended to prevent the online collection of personally identifiable data from children under age 13. The U.S. Federal Trade Commission (1999) has issued basic rules on what online businesses must do to comply with this regulation. In general, the FTC states that if a site directs service to children under 13 or knowingly collects knowledge about children under 13, they must comply with the law and must post a privacy notice and receive verifiable parental consent to collect a child's information. This legislation would affect any online Internet pharmacies that dispense information to underage children.

In April 2001, the FTC (U.S. Federal Trade Commission, 2002b) surveyed 144 Web sites directed at children 12 and under. The survey showed that 72% of the sites collected personal information online, such as the child's full name and email address. The study came to two conclusions about the state of Web sites following COPPA law. First, most sites are complying with the requirement that they identify to the user that they are collecting children's personal information. Second, other COPPA specifications are not followed consistently, such as compliance with how this information is used (U.S. Federal Trade Commission, 2002b).

Changes to Policies

Online Web firms may notify consumers of changes to their privacy policies. In order to alert consumers, a caveat within the policy page indicates a policy may change

and that notices to specific changes to the policy are available on the Web site. Many leading firms have posted changes to their sites notifying consumers of changes. Hu (2003) provides two examples of prominent firms posting changes to their policies, Disney and Yahoo. Disney changed its privacy policy in late 2003 to allow sharing of customer information with outside firms. Customers now must take the initiative to opt-out of this sharing provision.

Pharmacy Licensing and Written Prescriptions

One factor online consumers can use to evaluate the authenticity of both Canadian and U.S. Internet pharmacies is whether the pharmacy holds a valid license. However, before customers review the privacy policies and licenses, they must understand the type of online firms with which they are dealing. According to PharmacyChecker.com (2003d), there are two types of online pharmaceutical firms, pharmacies associated with brick and mortar firms, and pharmacy intermediaries. The latter type merely serves to fill orders through an associated pharmacy. PharmacyChecker.com (2003d) states that U.S. firms are required to be licensed in the state to which they ship their products. This makes it easier for consumers to take legal action if they encounter troubles. However, because drugs purchased through U.S. online sites are considered expensive, consumers are flocking to Canadian-based online pharmacies and intermediaries. According to studies by the U.S. Congress House of Representatives Government Reform Committee, U.S. citizens pay an average of twice as much for the same prescription drugs as citizens in other countries, and can pay up to 10 times more for certain drugs (U.S. Congress, House, 2003).

Those consumers who utilize specific Canadian pharmacies may enjoy a higher level of protection when investigating if a site has a valid license. In 1999, the National Association of Boards of Pharmacy (NABP) in Canada created the Verified Internet Pharmacy Practice Sites (VIPPS) program to provide consumers with the ability to use a single source to check a pharmacy's certification (National Association of Boards and Pharmacy, 2004). The VIPPS program certifies pharmacy sites as having legitimate licenses and as having undergone a certification process. If an online site has a VIPPS certification icon on its site, consumers have a way to verify licensing. However, as of January 2004, only 14 pharmacies, mostly large national U.S. pharmacy chains, meet the VIPPS qualifications, compared to the myriad of current Canadian online pharmacies (National Association of Boards and Pharmacy, 2004).

Another issue to consider is whether the site requires a written prescription from a physician. Although Canadian law states that physicians must sign Canadian prescriptions, the standards for pharmacists in each province differ, which can lead to the possibility of online pharmacies bypassing professional standards (Whitwham, 2003a, p. 759).

Opt-in and Opt-out Strategies

Cadogan (2001) proposed that an opt-out strategy might be better for merchants and consumers than opt in. "This would permit businesses to better target consumers, while individuals would be better enabled to avoid invasion of their privacy" (p. 327). However, she conceded that many sources consider this impractical, expensive for businesses, and oblivious to the fact that consumers are opting in even before they make a purchase, either by filling out information forms or simply by visiting the site.

Cadogan's (2001) strongest recommendation is that consumers need comprehensive and accurate information if they desire to protect their privacy. She recommends that consumers gain knowledge of security and technical issues as well as marketing and technical issues. Lee (2002) shares a similar perspective. Both authors recommend providing information to the public that covers technical issues related to privacy but is easy for the layperson to comprehend. They also note that online privacy is a global issue, thus a more uniform privacy program would be the most practical approach. In fact, Cadogan (2001) suggests pressure from the European Union will inevitably lead to more uniform international privacy policies. Cadogan also argues that online businesses have a large stake in upholding the privacy wishes of consumers for two key reasons. The first is the issue of winning consumer trust. A second reason is that complaints about privacy abuses could lead to government regulations that fail to consider the dynamic nature of cyberspace and thus have the counterproductive effect of stifling Internet commerce. If Internet firms do not police themselves and provide strong privacy, then legislation may be passed that would benefit consumers, but may not be friendly to online firms.

A 2001 survey on the privacy policies and practices of commercial Web sites synthesized data from the 85 busiest Web sites ("most popular"), a random sample of all sites with more than 39,000 unique visitors, and a subset of the random sample that focused on the top 5,625 sites (Adkinson et al., 2002). The study marked the fourth in a series of research projects beginning in 1998. The 2001 study found that Web sites were gathering less information than they had two years earlier, showing a steady rate of decline. The researchers also observed fewer Web sites with third party cookies, dropping

to 48% from 78% for the most popular sites and to 25% from 57% for the random sample. Consistent with this trend, they also noted that privacy notices were more prevalent and more prominently displayed. Virtually all the most popular sites and 83% of the random sample had privacy notices, roughly the same as for 2000. While the privacy notices tended to be more easily accessible, they were lengthier.

An interesting change was the reversal of Cadogan's (2001) finding that opt-out policies were more prevalent than opt-in policies. In the sites included in both the most popular category and the random sample, Adkinson et al. (2002) reported a marked decline in the number of Web sites with opt-out polices and a marked preference for opt-in policies. The researchers also found more sites offering a better combination of fair information practice components. The only finding that did not appear to differ substantially from the previous study was the use of P3P enabled browsers and privacy seals. The use of privacy seals clearly lagged far beyond other privacy protection practices.

At the time of the study, P3P technology had only been available for a short time. However, Adkinson et al. (2002) noted that 25% of the most popular Web sites and 5% of the random sample had implemented the protocol, which they considered a good start. The World Wide Web Consortium (W3C) Platform for Privacy Preferences (P3P) is a standardized method that enables Web sites to encode their privacy policies in a computer readable format (W3C, 2003). P3P was in the development stage for several years, and the development of the technology has been controversial (Hochheiser, 2002).

Flammia (2000) proposed that, "If most Web sites agree to publish privacy policies and seals of approval in machine-readable format, they pave the way for

distributed intelligent agents that could act on our behalf and protect our privacy." Although somewhat ambivalent about the thought of "distributed intelligent agents" protecting consumer privacy, Flammia noted that it would shift the burden of scrutinizing privacy protection from the consumer to the technology (p.13). Hochheiser (2002) refers to P3P as a "social protocol," which has been criticized as a mechanism that allows online business to escape meaningful legislation. The W3C counters that the purpose of P3P technology is providing consumers with more control over their personal data (W3C, 2003). Depending on one's perspective the rapid adoption of P3P technology by Internet sites, particularly the most heavily trafficked, may either be construed as evidence that Web businesses are responding to consumer demands for control over their personal data or attempting to avoid additional regulation. The findings reported by Adkinson et al. (2002) suggest that Web businesses are responding to consumers' privacy preferences. According to W3C (2002), about 25% of the top 100 Web sites have adopted P3P. However, adoption since 2002 had slowed due to the state of the economy and downsizing of privacy staff.

Consumer Behavior

There is a dichotomy between consumers expressing a desire for tight privacy policies, yet still utilizing online firms that do not adhere to these ideals. Several studies have validated this discrepancy in consumers' privacy desires not matching their behavior when deciding whether to use the sites.

Hsu (2003) conducted a cross-cultural study of Internet privacy issues that encompassed regulations, Web site privacy statements, and the attitudes of consumers in China, the Netherlands, Taiwan, and the U.S. An intriguing finding was that there seemed

to be little connection between consumers' concern for privacy and their personal practices. He found that even if customers are significantly concerned about the privacy of their personal data on a specific Web site, they will still disclose large amounts of personal information. Although the participants from the two Asian countries reported more concern with privacy than those from the two Western countries, the Chinese and Taiwanese subjects disclosed *more* information than their Western counterparts. Another interesting point of the study was that out of 400 respondents, only *nine* clicked on the Web sites' privacy policies.

The context of the Web site emerged as an important factor in consumer's decision to disclose information. The Taiwanese and Chinese respondents placed their greatest trust in government sites and the Dutch respondents disclosed a substantial amount of information to government Web sites (Hsu, 2003). For the Americans, the pattern showed that they were most cautious about disclosing information to government Web sites but gave far more information to commercial Web sites than respondents from any of the other three countries. Both Asian samples gave more information to community Web sites than either Western group. All the respondent groups kept health information private although Hsu noted that health information was irrelevant to the sites visited. Therefore, disclosing health information, as with other information, would be largely a factor of culture and context. This study also showed that consumer practices are dynamic and change depending on a myriad of factors, including demographics of the user, the type of Internet site, and governmental involvement in privacy issues.

A second study by Earp and Baumer (2003) corroborates Hsu's observations. They surveyed 415 consumers about their opinions of 1 of 30 Web sites. These sites were

equally divided among retail, financial, and health/medical sectors. Each category contained 15 well-known and 15 lesser-known Web sites. The participants were asked what types of information (demographic, personal, medical, and financial) they were willing to disclose to the sites. In general, the participants were most willing to disclose age and gender and least willing to reveal their social security numbers. They were least reluctant to provide personal information to health sites, followed by financial sites, and least of all to retail sites. The respondents expressed greatest reluctance to providing personal information to unfamiliar sites. They also inferred that consumers are more willing to trust well-known sites because of perceived legal protection of their information on these familiar sites.

Earp and Baumer (2003) found some differences when they compared the responses of subjects aged 15-35 and those over age 35. The younger respondents were more prone to provide their name, age, and gender; to read the Web site's privacy policy; and to provide information in exchange for material incentives. The older respondents were more apprehensive about identity theft, losing control of their information, unauthorized dissemination of personal information, and exposure to dishonest people. These differences suggest that both age groups were aware that their privacy could be compromised on the Web. However, the younger respondents were savvier about privacy policies, which enabled them to reveal information more comfortably. However, the older respondents seemed to have more of a global distrust of disclosing information online.

These studies indicate that online users have conflicting emotions and practices between their views on privacy versus their actual usage of the sites. Although consumers express a strong desire for online firms to protect their privacy, other factors can

overwhelm their desire for information protection. Some factors depend on the consumers themselves, such as upbringing and age. In short, Hsu (2003) found privacy concerns do not translate to comparable actual practices for consumers.

Consumers recognize that in order to obtain shopping convenience and cost savings, they may be required to sacrifice a level of privacy. J. Howard Beales, Director of the FTC's Bureau of Consumer Protection indicates that consumers recognize these trade-offs in the commercial arena. He states that consumers are willing to make compromises between absolute privacy and economic benefits (U.S. Federal Trade Commission, 2004). Consumers may also view other factors on online sites as more important than privacy policies. Cost savings, proper licensing, and comprehensive prescription information may constitute a trade-off to an effective privacy policy. It is important to review these other factors to determine a customer's willingness to utilize a site.

Health Information on the Web

Privacy Policies

In view of the record amounts of information consumers are providing to health-related Web sites, the California Healthcare Foundation conducted a survey of privacy policies and practices of 21 heavily trafficked health-related Internet sites (Goldman et al., 2000). The sites represented a spectrum of categories: sites where consumers' wishes for privacy might be more important, sites where consumers were researching and purchasing health products and pharmaceuticals, general search engines or portals with substantial Internet traffic, and sites targeting a specific demographic. The study was conducted in two ways. First, the researchers reviewed sites' stated privacy policies

against a set of "fair information practice principles," which were previously explained in the *Fair Information Practices* section of this study. Second, the researchers played the role of a typical visitor to each site to observe and capture the information they submitted. The study reviewed privacy policies on these sites and compared their written policies to their practices.

Even when online firms include privacy policies on their Web sites, the features in the policies differ widely among firms, and they may not adequately protect user data. Goldman et al. (2000) reported several findings, some ubiquitous to the Internet and others specific to health-related sites. The first is a problem across the Internet: users are unaware that their personal data is being collected and their visits to Web sites are not anonymous and are tracked. Using mechanisms such as cookies, profiling, and banner ads, firms can gather information about consumers and their surfing habits. Second, most sites adhered only nominally to fair information practices. Although most of the studied sites posted privacy policies, few did an adequate job of safeguarding users' personal healthcare information. Few met adequate privacy criteria such as providing sufficient notice, providing users with control over their information, and holding business partners to the same standards of privacy. Thus, it is not surprising that the researchers observed discrepancies between the privacy policies of the health sites and their practices. A common practice included collecting personal information via cookies and banner advertisements by third parties without indication by the host sites. Few of the sites had a partnership in which third parties were held to the same privacy standards as the host site. Goldman et al. (2000) also noted instances involving the transfer of personal information of third parties in explicit violation of privacy policies.

Failure to disclose collecting personal data through cookies and banner ads and transferring personal data to third parties in violation of privacy policies were two of the primary problems Goldman et al. (2000) found on the health-related Internet sites. A third problem was inadequate security that raised the risk of unauthorized access to visitors' personal data. Goldman et al. (2000) acknowledged that given the rapidly changing nature of the Internet their findings are probably subject to change over time (in fact, several of the Web sites no longer exist). However, their recommendations to Internet health sites are equally valid today. They recommended that health sites make greater attempts to provide visitors with anonymity, close the gap between their privacy policies and practices, and of particular note, work collaboratively to develop a model privacy policy for Internet health sites.

Consumer Attitudes and Behavior

The Pew Internet & American Life Project, a nonprofit initiative dedicated to researching the impact of the Internet on various aspects of American life, conducted a series of studies in early 2000 related to consumer use of health-related Web sites and the consumers' attitudes toward privacy issues. The samples were derived from the larger study of Internet use. For the first exploration of health seeking on the Web, the researchers contacted 2,109 adults, including 1,101, who were Internet users (Fox & Rainie, 2000). A sub-sample of this group consisted of 521 Internet users who sought health information online.

Fox and Rainie (2000) found a small percentage of adults who used the Internet for consulting a physician or purchasing medications or vitamins online. Of this sample, 17% had given their name or other personal information to a health site and 21% had

provided their email address. More than half (54%) had gone online on behalf of someone else on their last health site excursion, including children, parents, other relatives, or friends; only 43% said they had visited the site for themselves. A majority was seeking information about an immediate medical problem, primarily in conjunction with a doctor's visit. The vast majority (93%) appreciated that they could get information on the Web at their convenience. Most agreed that the Web offered more health information than they could find anywhere else (83%). A similar proportion cited anonymity as important (80%), and 16% of respondents said they used the Internet for information dealing with a sensitive health issue about which they found it difficult to talk.

The preference for anonymity was accompanied by apprehension about privacy breaches on the Web (Fox & Rainie, 2000). The overwhelming majority of respondents (89%) were concerned that an online site might sell or give away information about their visit; 71% said they were "very concerned." A major concern was that they might be denied insurance coverage or have their insurance rates increased because of the health sites they browsed (85%), with 72% describing themselves as "very concerned." Slightly more than half (52%) were afraid their employers might find out (this concern was less prevalent since most respondents were going online at home). The respondents were divided over the merit of putting medical records on the Internet, although a majority of health seekers (63%) as well as Internet users in general (60%) thought it was a bad idea. They were concerned about people gaining access to their personal medical files even on a secure, password-protected site. The rest of the sample favored putting medical

information online because it made it easy for them and their doctors to access the information.

Demographically, Fox and Rainie (2000) found a higher proportion of women than men using the Internet for health information (63% versus 46%, respectively). Neither income nor ethnicity predicted use of the Web for health information, in contrast to findings from research on other online activities. The highest proportions of health seekers fell into age categories between 30 and 64. Internet experience had some effect on seeking health information online, although the researchers noted the difference between novices and experienced Internet users was smaller than for most online activities.

Almost half the respondents who sought medical information online (48%) reported the information they found on the Internet helped them to take care of themselves and 55% said the Internet offered a better way to gain health information. However, Fox and Rainie (2000) noted that most were concerned about the legitimacy of the source. Among all Internet users, whether or not they sought medical information online, 82% were concerned about getting unreliable health information online. As a result, 58% were careful to check the name of the organization providing advice on a health-related Web site. This practice was more prevalent among respondents who had at least some college education.

Overall, the findings of the 2000 Pew study (Fox & Rainie, 2000) showed both caution and concern. Despite apprehensions about privacy breaches, and to a lesser extent unreliable information, Internet users welcomed the ease of access to health information offered on the Web and roughly one-half reported positive health benefits.

A subsequent Pew study delved into the privacy concerns expressed by the overwhelming majority of respondents. The researchers noted that there is a double-edge to both paper-based and electronic medical databases (Choy et al., 2001). The tasks involved in locating and distributing paper files limit the chances that the data will reach unauthorized sources but may also limit information access and sharing by legitimate stakeholders. The concerns over electronic data files are exactly opposite. Information is easy to obtain for legitimate purposes but the ease of access raises the risk of unauthorized use.

Choy et al. (2001) addressed the extent to which the activities of Internet health sites fall under the jurisdiction of HIPAA. Generally, HIPAA applies only to three health care entities: health care providers, health plans, and health care clearinghouses. This limitation excludes many health-related Web sites. Thus, depending on who owns or operates the Web site, a site offering the same services may or may not fall under the heading of a "covered entity." The Pew study examined the nature of different types of health sites on the Web and the degree they were covered by HIPAA privacy regulations.

Choy et al. (2001) found a large gray area in the nature of health-related Web sites that sell multiple services. For example, some Internet sites that dispense health information also allow patients to review test results online. This latter service falls under the privacy regulation, while most of the communication on the site probably does not. Another example is drugstore.com and the online services portions of pharmacies such as CVS and Walgreens, which sell both prescription drugs and non-prescription items online. The prescription drugs are protected under the privacy policy; the other items are not. Choy et al. (2001) suggest that posting privacy practices may complicate the privacy

issue by confusing consumers and possibly leading consumers to believe all their transactions are covered under HIPAA. The prevalence of health sites that perform multiple services highlights the importance of posting a privacy policy that is clear, accurate, and easily understandable to online consumers.

Internet sites that are entirely under the control of patients are excluded from privacy regulations. Choy et al. (2001) note that this has the effect of patient-controlled health sites allowing patients access to information, yet, visitors may be unwittingly relinquishing control of their health information by providing it to the sites that are exempt from the policy. There are also Web sites that allow visitors to create their own medical records online. If they are not owned or operated by covered entities, the privacy of these records does not fall under federal regulatory oversight.

Overall, the Pew researchers found serious limitations to the extent that health-related Web sites are covered by regulatory mandates. The HIPAA rule, which covers only health plans, health care providers, and health clearinghouses "may create an illusion of legal protection that may lull consumers into a false sense of security when they engage in online health activities" (Choy et al., 2001, p. 24). The report concluded that

> People often believe they are invisible and anonymous online, but they are often exposing their most sensitive health information and online health sites that are not required by law to protect the information or keep it confidential. The potential for abuse is enormous. (Choy et al., 2001, p. 25)

The 2000 Pew study provided a general picture of U.S. consumers' reliance on the Internet for health information. A second study conducted in late 2002 provided a

more detailed analysis of online health-seeking behaviors. This study involved 2,038 adults, including 1,220 Internet users (Fox & Fallows, 2003). Searching health sites online proved to be one of the most prevalent online activities. Eighty percent of the sample, or roughly 93 million U.S. adults, reported searching for information on one of 16 health-related topics. As in the 2000 study (Fox & Rainie, 2000), the largest segment of health seekers used the Web to find information about a specific medical condition (63%), followed by researching a particular medical treatment or procedure (47%). Roughly one-third (34%) of the sample sought information on prescription or over-the-counter drugs (Fox & Fallows, 2003).

More women (85%) than men (75%) sought health information online (Fox & Fallow, 2003). However, 80% of the respondents who reported visiting health-related Internet sites said they did so infrequently (every few months or even less often). Only a small proportion reported communicating with doctors online or through e-mail, although those who did regarded it as a convenience. Doctors seemed to have mixed feelings about seeking health information online; some supported their patients' online health seeking, while others advised against it. The authors found that the proportion of respondents who held high regard for the Internet for improving the health information and services they received jumped from about 50% in the 2000 survey to 73%. Respondents offered suggestions for improving access to health resources on the Web although in some cases the information they sought was already available online, albeit without clear links for finding it.

Most of the 2002 findings reiterated the results of previous research. However, despite the increasingly positive attitudes of consumers toward online health resources,

Fox and Fallows (2003) noted that only a minority followed recommended search guidelines. Only about one-quarter were meticulous in checking the source and timeliness of information or verifying the information they found each time they conducted a search. Another quarter said they checked the source and date of a site's information "most of the time"; half did so "only sometimes," "hardly ever," or even "never." In general, the respondents were largely satisfied with the health resources they found on the Web, particularly individuals with disabilities or chronic illnesses and those in rural areas whose Internet access to health information was greatly improved.

The most recent of the Pew studies focused specifically on consumer behavior regarding prescription drug information. The sample consisted of 2,200 adults, including 1,399 Internet users, interviewed in spring 2004 (Fox, 2004a). The huge market for prescription drugs was confirmed by the finding that 64% of the households surveyed consume prescription drugs on a regular basis. However, the proportion of adults who have searched for prescription drugs online is low; 21% personally conducted a search and 5% had someone else search for them. The groups most likely to have conducted prescription drug searches online included individuals with high-speed Internet access at home and at work, Internet users with six or more years of online experience, college graduates, and Baby Boomers. The practice was most widespread in the 40-49 year-old demographic and least common among seniors age 69 or older. Individuals with chronic illnesses or disabilities were no more predisposed than other groups to search for prescription drugs online, although Fox (2004a) noted that others might have conducted such searches for them. While seeking generic health information online cut across all ethnic backgrounds (Fox & Rainie, 2000), white consumers were about twice as likely to

seek prescription drug information as blacks or Latinos (24%, 12%, and 14%, respectively (Fox, 2004a).

In Fox's study, the respondents displayed considerable skepticism about buying prescription drugs online; 62% believed it to be less safe than purchasing drugs from a local pharmacy (Fox, 2004a). Only 20% considered the two venues equally safe. A substantial majority (68%) agreed with the statement, "Some argue that allowing people to purchase prescription drugs online makes it too easy to obtain drugs illegally, without a prescription" (Fox, 2004a). Furthermore, 71% agreed with a statement that people should not be allowed to purchase prescription medications online because drugs purchased from pharmacies outside the U.S. lack the safety guarantees of pharmacies licensed within the U.S.

Fox (2004a) noted that some respondents came from states where legislators encouraged residents to purchase drugs less expensively from Canadian pharmacies. Indeed, the report contained Minnesota governor Tim Pawlenty's famous response to federal concerns about the safety of Canadian drug imports, "Show me the dead Canadians" (p. 5). Nonetheless, only 4% of the Pew respondents reported buying prescription drugs online (3% for personal use and 1% for others). This group included a small number of non-Internet users. While lower cost is the most widely cited reason for purchasing drugs online, the practice is more common among consumers that are more affluent.

The most prevalent reasons for ordering prescription drugs online from both Canadian and U.S. pharmacies tended to be convenience and time- and cost-efficiency (Fox, 2004a). A similar majority described themselves as "very satisfied" with the quality

of the drugs they bought and the customer service they received; about 50% were "very satisfied" with the price. Not surprisingly, given the high satisfaction, 90% said they would fill prescriptions online again.

Summary

The quest for lower cost drugs on the Internet by American consumers takes place in an atmosphere where a large amount of information changes hands on a daily basis. Consumers have access to information that enables them to take better care of their health. However, this often comes at the cost of concerns over the privacy protection of sensitive personal information.

Theoretically, online consumers engage in a cost-benefit analysis, typically deciding that the convenience, ease, and time- and cost-efficiency of Internet purchasing justify the potential cost of misuse of personal information. A sizable proportion of Internet users are unaware that the "anonymity" of cyberspace is an illusion or they are unaware of the steps they can take to protect their privacy. Over the past two years, online businesses have decreased the use of third party cookies and sharing consumer data with business partners, in recognition of the preferences of consumers. These actions reflect the preference for self-regulation that has historically governed U.S. commerce.

The intense debate over Americans' purchase of prescription medicines from online Canadian pharmacies has many unique problems and issues, and it reflects the larger issues of privacy and trust in Internet commerce. Paradoxically, by limiting American access to Canadian drugs (which are frequently made in the U.S. and then re-imported from Canada), the pharmaceutical companies may be raising the risks to consumers of imported drugs by exposing them to drugs manufactured in countries that

lack the stringent regulations of Canada and the U.S. Despite the highly charged issue, however, only a small proportion of U.S. consumers buy prescription medicines online. Drug quality is one issue cited by prospective consumers. However, the literature to date suggests that privacy protection is an overarching concern of Internet users, and is likely to inhibit widespread growth of Internet drug purchases for both Canadian online pharmacies and legitimate U.S. online pharmacy firms even when it results in substantially lower cost.

Chapter 3

Methodology

Introduction

This chapter presents the methods and procedures used to develop the surveys of privacy polices among Canadian online pharmacies and consumer usage of these sites. A discussion of the procedures, evaluation tools, and instrumentation will be emphasized. There are two phases used to develop the evaluation tools. First, a review of specific privacy factors contained in the online sites was compiled and analyzed. The second phase was to develop an online survey defining how users of medical Web sites view Canadian pharmacies. This chapter concludes with a review of the reliability, validity, and assumptions.

Research Methods Employed

For the initial phase of this study, a systematic review of 25 online Canadian pharmacies was undertaken. These pharmacies were chosen from two listings. The first half of the pharmacy list was chosen randomly from Canadian Online Pharmacy Directory (2004), an online Web site service that aids Americans in locating Canadian online pharmacies. This is a business directory that lists 127 large Canadian pharmacies that have paid to be included on a consumer portal Web site. Thirteen pharmacies from this list were randomly chosen by the researcher. The other portion of the list was gathered from a search of Google.com. The keywords “Canadian online pharmacy” was used to search for a variety of these firms, and the second portion of the research list was

gathered from this query. Although other search terms could have been utilized, these keywords form a popular basis for the overall conditions of this study. In addition, the results were chosen from only the search results, not from the results of any sponsored links. The researcher chose the top 12 pharmacies from this source. From these two sources, a final list of the 25 Canadian pharmacies was chosen for the study (see Appendix A).

Based on the pharmacies chosen for this study, an in-depth review of specific privacy policy pages and procedures followed. Because sites change their pages and information, privacy information that the reader may review in the future may be different than the results gathered from this study.

A technical issue encountered in preliminary analysis by the researcher in assembling this methodology was the dichotomy between the privacy policy information posted on the site versus the actual practice of the firm. For example, the privacy policy page might not mention that the site collects customer email or telephone information. However, a sign-on page on the site could require this information, although this collection was not specified in the privacy statement. Thus, there was a quandary on whether to include information collected throughout the site, but not mentioned in the privacy statement. Due to the scope of this study, the decision was made to concentrate on information specifically contained within the privacy policy.

The second phase of the study involved an online survey of users of medical Web sites and their views of Canadian online pharmacies. The audience consisted of consumers who utilize medical information sites and were willing to take an online survey. The subjects were recruited from consumers utilizing one of several consumer

medical sites including (a) DrKoop.com, (b) HealthCentral.com, (c) MDchoice.com and (d) HealthScout.com. The study analyzed both users and non-users of Canadian online pharmacy sites, and determined what issues were major factors in why consumers choose to utilize these firms, including privacy policies, cost, or quality.

There were some issues encountered when picking the medical sites to use for serving as the portal to the online survey. In order to use a medical site as a portal, a text link was placed on the medical site as an advertisement. This link invited respondents to click on the link in order to complete a survey about online Canadian pharmacy usage. A screen print of one of the advertisement text links on Web site healthcentral.com is found in Appendix D. A text link to the pharmacy survey is displayed in the middle of the screen print. When the initial contact was made with representatives of several other medical sites, such as WebMD.com, the researcher was informed that these sites would not accept advertisement links for surveys. This research was thus limited to medical sites that would accept survey advertisement links.

There were several reasons why the four health sites noted above were chosen. First, all of these sites used the same advertisement firm, GoText.com, to place advertisements on health-care portal sites. This advertisement firm allowed the researcher to submit text advertisement links to the Canadian online survey. Second, these health Web sites are leading distributors of health and medical information to a large number of Internet visitors. MDchoice.com acquired both HealthScout.com and HealthCentral.com in 2001, although these three still run independent Web portals. Together, the firms attract more than 1.5 million visitors each month and are one of the five largest U.S. online health networks (MDchoice, 2001; HealthCentral.com, 2001). DrKoop.com is

named after former U.S. Surgeon General, C. Everett Koop, M.D., and is chairman of the board of the company operating the site. Prior to filing bankruptcy in December 2001, DrKoop.com attracted more than 900,000 visitors per month and had a database of more than 2 million registered users (Cox, 2002). Although the number of visitors has diminished since the bankruptcy, it still has a sizable audience with an average reach of 60 visitors per million who visit the Web. It ranks 22,903 in most visited Web sites. HealthScout.com ranks 26,707, HealthCentral.com ranks 14,115, and MDchoice.com ranks 46,022 as of March 2005 (Alexa Internet, 2005).

The second phase of the project involved a survey of medical sites. The survey consisted of 44 questions divided into nine specific sections based on the following criteria (a) demographics, (b) overall privacy policy, (c), consumer/licensing, (d) personal demographic information, (e) cookies, (f) opt-in/opt-out/update ability, (g) third party disclosure, (h) security, and (i) miscellaneous.

A Likert scale technique was used to measure participant's attitudes. Each of the 44 questions was given a ranking on a scale of 1 (strongly disagree) through 5 (strongly agree). In addition, there was also a "not applicable" ranking for those respondents whose experience with a question did not constitute a rating. A review of the questions can be found in Appendix C of this study.

Location of Online Study

The online survey was hosted on a Web site coordinated by www.hostedsurvey.com. The questions were consolidated into a single Web-based survey hosted by this firm. Survey results were collected into a database hosted within this site for further analysis. In order to access this Web-based survey, users clicked on a

text link that connected them to the questionnaire. A text advertisement marketing group (GoText.com) handles banner click-throughs for a variety of medical sites. This firm placed the text links on four consumer medical sites (a) DrKoop.com, (b) HealthCentral.com, (c) MDchoice.com, and (d) HealthScout.com.

Subjects of Online Study

The first group of subjects (for the initial testing of the survey instrument) was a group of 10 students recruited from an e-commerce class the researcher was teaching at St. Petersburg College in Clearwater, Florida. The second group of subjects in this study were recruited from a random sampling of customers utilizing the four medical sites. These are sites that specialize in healthcare issues and provide consumers with medical information. The subjects were expected to be online consumers who have specific health concerns, and thus would be more inclined to utilize online pharmacies to purchase prescriptions. Customers of these sites were expected to be adults over 18 years of age, both men and women. There were 147 responses collected over a two-month period.

Methods and Procedures

For the initial test, approximately 10 students from the aforementioned e-commerce class were asked to take the survey. The results were used to determine the validity of the test questions and to ensure that the technology, Web site, and survey functioned properly. During a regularly scheduled break, the students were asked to volunteer to take this short survey. The length of time for taking this survey was between 10 and 15 minutes.

The subjects for the second, main phase were recruited from consumers utilizing one of several consumer medical sites including DrKoop.com, HealthCentral.com, MDchoice.com, and HealthScout.com. A text link was placed on each of these sites that contained a Uniform Resource Locator (URL) where a survey was found on www.hostedsurvey.com.

Each subject was asked to take a short survey containing 44 questions dealing with their views and experience with online pharmacy sites. The survey consisted of the questions found in Appendix C. Survey results were placed in the database for www.hostedsurvey.com, and was only available by the researcher via an ID and a password. No other person had access to the individual un-aggregated data, thus ensuring data security.

Instrumentation Development and Dissemination of Research Instruments

The literature review aided in the development of the research questions to ask in a survey of sites. The literature was used to first aggregate a number of general privacy policies that should be contained on any Web site. Then, additional literature was researched to include privacy policies specific to the online pharmacy industry A compilation of both general policies and pharmacy-specific guidelines was generated in order to review them against the policies for 25 major online sites. In addition to the literature review, Pharmacycheck.com (2003c) conducted a small study of sites for a limited number of factors when evaluating privacy policies for Canadian online pharmacies. This research expanded that study to a more comprehensive assessment of each of the 25 sites chosen for this study.

Site Surveys

The development process for this study began by compiling a list of privacy policy procedures that could be contained on a firm's privacy policy site. A list of policies was compiled and categorized into main sections. Appendix B features a spreadsheet listing the 25 online Canadian pharmacies on the top columns. The left rows detail main sections of privacy policy facets that will be further explained in the subsequent sections of this study. The researcher reviewed the privacy policy on each site to determine which particular privacy functions were listed on the site. Gaps in the privacy policies for a specific site were compared to overall specific policies that the firm could include in a policy, but may have chosen not to include. This study only analyzed which personal data the site indicated that it captured, and did not investigate the firm's storage, dissemination, protection, or destruction of the consumer data.

Overall privacy policy

A site can contain an overall privacy policy page that could be accessed in a variety places throughout the Web site. Ideally, a privacy page link should be found at the bottom of the index (or home) page of the site for ease of access. Links to the privacy page could be found on other non-home pages but may present difficulties in consumers finding the page. This study determined if an online pharmacy site contained a privacy policy page, and where on the site it could be accessed.

Privacy seal use

Online pharmacy sites can use independent third-party organizations such as TRUSTe and BBBOnLine in order to enhance consumer confidence in overall operations

as well as their privacy policy. In order to use the reliability seal of approval, an e-business must adhere to established privacy principles promulgated by these third-party organizations. Sites that hold sway to the principles of these seal programs may have the privacy seal icons on their site, and the research analyzes if pharmacy sites use either of these seals. Online sites often place these privacy seals on the home page, but it is conceivable they may be found on other pages. The study determines if two of the most common privacy seals (TRUSTe and BBBOnLine) were found within the sites.

Demographic information

Sites can collect a variety of information about their customers, some of which may be required by the pharmacy and other data that the user optionally chose to divulge. This research analyzed whether the privacy policy revealed if the site collected the following demographic information: email, address, social security number, telephone, credit card, and demographics (age and gender).

Medical information

Sites can collect a variety of information about their customers, some of which may contain highly personal and confidential data. The study reviewed whether the site's privacy policy indicated whether medical information was collected and kept confidential.

Use of cookies

Cookies are small text files, placed on a user's computer by the site's server programs. Sites use cookies for a variety of reasons, such as saving login information (such as user ID and password) to provide for quicker logins. Previous login session

information may be saved in cookies for use in subsequent sessions. For example, an online pharmacy site could place a cookie on a consumer's computer the first time the customer signs into the site to purchase a prescription. When a consumer subsequently desires to purchase pharmaceuticals and signs into the site, the cookie could contain the user's ID and password for faster login. If a site uses cookies, the usage policy may be included in the privacy page so users understand the reasons for their use, and how cookies may benefit them. This study examined if a site disclosed its cookie policy on the site.

Computer hardware and software information collect from cookies

Firms collect a variety of information about users and store this data in cookie files. Surfing patterns can be used to help keep track of popular and rarely used pages, thus providing the site operator with data useful in making beneficial changes to these pages. This study assessed the following hardware and software information that sites collected: Internet Protocol (IP) address, browser types, referring Web site address, log files, usage tracking, and domain name.

Opt-in and opt-out

Online marketers have two tactics for permission marketing: opt-in and opt-out. Opt-in refers to a consumer taking voluntary action to receive something; it is initiated by a consumer. Opt-out refers to the ability to decline further services, such as email. In opt-out, a consumer may have voluntarily signed up for a service, and then later decides not to use the service, thus "opting-out." In addition, online vendors may acquire email listings and send spam to consumers. If consumers no longer wish to receive the notices,

they must follow the opt-out procedures. It should be noted that Canadian law requires an opt-in while the U.S. approach is opt-out. (Canada Privacy Commissioner, 2003b, para. 4) Each option was analyzed in this study.

Personal update of information in system

Because of changing consumer medical and personal data, it is critical for these sites to provide their consumers with the ability to update and delete personal information, especially medical records that can have an effect on health. Three update options were analyzed. First, the study determined if the privacy policy stated that consumers could delete information from the site. Next, the site was analyzed to ascertain if the privacy policy reveals whether users can delete archived information. Finally, the research ascertained if a consumer could update information in the site's database.

Disclosure of information to third parties and affiliates

A privacy page may contain disclosure information that indicates if the hosting site reveals personal information to third party entities or affiliates. This dissertation began by determining if the site indicated whether it disclosed data to third parties and if the customer had the ability to consent to this action. Next, statistics were gathered indicating whether the site disclosed data if required to perform services, if legally required, if the firm is acquired by another, or if the site shared information with affiliates.

Steps firms take to provide security

The safety of personal information is one concern of consumers when reviewing a site's privacy policy page. A common online security method is to provide login IDs and

passwords to users' account profile screen. Passwords are the initial barrier to prevent unauthorized access to personal information. Firewalls, SSL, and encryption techniques are other ways to secure data. At the firm's physical location, servers can be stored in a protected environment. In addition, only authorized company employees should have access to the data. This study evaluated the site's policy page to determine what security processes and methods were utilized.

Absolving data collection

When consumers post their medical and personal information to a pharmacy site, that information will be used by that specific online firm. However, it is conceivable that unethical firms or individuals could collect information and use it for dubious means. Thus, it is imperative that online sites disclaim any intention of inappropriate use of a consumer's data by third parties. An analysis of the policies revealed if the site rejected third-party data collection.

Collection of data from children under 13

The U.S. Children's Online Privacy Protection Act (COPPA) was designed to thwart the collection of personally identifiable information from children without their parents' consent. Although it is highly unlikely that any child would need to use the services of an online pharmacy site, it would still be advantageous to indicate that the site complies with U.S. law because of the number of U.S. consumers who use the site.

Will post changes to privacy policy

As business requirements and laws change, a company should periodically review its privacy policy. If the firm modifies its policies, updates should be posted to the privacy page, thus keeping consumers up-to-date with guidelines.

Provides email or phone contact on privacy page

Online consumers may pose questions about the firm's privacy policies and statement, and may desire clarification. Therefore, contact information should be provided on the privacy policy page, such as a firm's phone number or contact email address. The research verified if sites used contact information on their privacy page.

Licensing

This research study analyzed whether the site contained licensing information about the pharmacy. An online pharmacy site could exist under one of three possible scenarios. First, it may not be licensed in either Canada or the U.S. Second, the Web pages may actually show a valid American or Canadian pharmacy license on the Web site. Third, the firm may function as a pharmacy intermediary, and have a third-party pharmacy fill its orders.

Research Approval

The project approval for the online consumer survey portion of this project was submitted to the Nova Southeastern University Institutional Review Board (IRB) for examination and approval. The project was accepted on December 20, 2004, and the IRB approval can be found in Appendix E.

Reliability and Validity

In order to assure the reliability of the online survey questions and to ensure that survey respondents correctly understood the process, the researcher conducted a short test of the survey questions with a pre-selected class of undergraduate students at St. Petersburg College. Allowing students to take the survey before the intended audience helped to establish that the questionnaire and the methodology were appropriate for this study. The students were asked to take the online survey of questions and were evaluated as a group as to the validity of the survey. Students were able to complete the questions within a 10-15 minute estimated time frame. The students were asked if they required clarification of any question, and if they understood the context of each of the questions. There were no issues associated with the survey.

After validation by a small sample of 10 students, the survey was made available to the consumers of the medical Web sites. In order not to annoy consumers with a lengthy questionnaire and to increase the likelihood that all questions were completed, it was decided to keep the survey to 44 questions that could be completed in 10-15 minutes. Because all the pretest respondents were able to complete the survey within this time, this should have validated that the larger group to be surveyed should also have been able to answer the questions within a similar time frame.

Assumptions

The medical Web sites chosen for the second portion of this study were assumed to contain a cross-section of consumers who were interested in medical issues, such as pharmaceutical concerns. The researcher presumed a certain portion of these medical site users used Canadian online pharmacies for their drug purchases, while the others used

more traditional channels of pharmaceutical distribution. It was further assumed that a random sampling of interested users would choose to take the survey. However, no controls were placed on these respondents to determine if their responses would be accurate. It is conceivable that some of the respondents could have been predisposed towards a certain bias, and may have answered questions based on their perceptions, not necessarily on their experiences. The possibility may also exist that strong user beliefs about privacy issues or beliefs in the issues of perceived high prices of drugs may have led users to skew the responses to questions in a certain direction.

Summary

This chapter summarized the research methodology that was used for two phases of this project: an online site evaluation and a user survey. The specific instrumentation was detailed as well as the specific procedures employed. Finally, the assumptions and limitations were reviewed in order to serve as an introduction to the results discussed in the next chapter.

Chapter 4

Results

Introduction

This chapter reviews the findings of an in-depth analysis of the privacy policies and procedures of 25 major online Canadian pharmacies, as well as the purchasing patterns and viewpoints of 147 consumers. The results provide information on consumer demographics, and the Web sites' overall privacy policy, consumer/licensing, collection of personal demographic information, use of cookies, opt-in/opt-out/update ability, third party disclosure, security, and miscellaneous characteristics.

Consumer Survey Analysis

Available through four Web sites (DrKoop.com, HealthCentral.com, MDchoice.com, and HealthScout.com), the online consumer survey collected data about the purchasing patterns and viewpoints of 147 consumers. The data were collected over a two-month time-frame. If respondents clicked the text link to enter the survey but did not actually start or complete the survey, the resulting data were not included in the results. The responses were collected via a survey hosting company, and the data were incorporated into an Excel file for analysis.

Consumer Survey Findings

Consumer Demographics

Nearly half of the respondents (n=66, 44.6%) were under 40 years of age, while 60 (40.5%) were age 41-60, and 21 (14.2%) were over age 60. There was an almost equal

division in gender (female: n=70, 47.3%; male: n=78, 52.7%). According to December (2005), a 2001 Pew study determined that the gender gap in Internet access has narrowed; for example, of the 104 million American adults with Internet access, just over half (50.6%) are women. As with the demographic question on age, the results of this survey do have a correlation with the average Internet user. Most participants (n=103, 69.6%) had an insurance plan. Of the 147 individuals surveyed, only 14 (9.5%) used an online Canadian pharmacy. Currently, only 4% of all U.S. consumers have purchased prescription drugs online (Resnick & Montania, 2003). This fits into the pattern of a low percentage of respondents indicating they had used online pharmacies.

Online Purchasing Factor Findings

Tables 1 through 10 show the frequency of respondents' answers to specific questions. For example, the left column on Table 1 shows whether the respondents have used an online pharmacy ("yes" response in left column) or have not used this type of pharmacy ("no" response in left column). The three columns to the right-hand side shows what the respondents answered ("yes" or "no") to the specific survey question. The "yes" column on the right-hand side of the table indicates a specific factor was important to the respondents, while a "no" response designates the factor was not important. For example, in Table 1, under the vertical "yes" column, 10 respondents who had actually used an online pharmacy viewed cost as an important factor in their online purchase.

Table 1 shows that 14 (9.5%) respondents answered portions of question series number 5 in Appendix C, indicating that they had purchased pharmaceuticals from an online Canadian pharmacy within the previous 12 months, while 133 respondents did not answer the series of question in this section. Ten (71.4%) of the 14 online buyers

answered question 5a (shown as "q5a" in Table 1 and "q*x*a" in subsequent tables in this section) and stated they considered the cost of pharmaceuticals available online before deciding whether to submit an online order. An interesting point was that although non-purchasers of pharmaceutical sites were not supposed to answer the question related to cost savings (question 5a in Appendix C), four respondents (3.0%) did respond that they would consider cost savings if they would eventually purchase from these sites.

Table 1. Frequency of Considering Cost for Online Purchases

		Cost		
Online		Yes	No	Total
Yes	Count	10	4	14
	% within online	71.4%	28.6%	100.0%
	% within q5a (cost)	71.4%	3.0%	9.5%
	% of total	6.8%	2.7%	9.5%
No	Count	4	129	133
	% within online	3.0%	97.0%	100.0%
	% within q5a (cost)	28.6%	97.0%	90.5%
	% of total	2.7%	87.8%	90.5%
Total	Count	14	133	147
	% of total	9.5%	90.5%	100.0%

Table 2 illustrates the importance consumers view privacy policies on a site when they have purchased from an online pharmacy. This relates to question 5b within Appendix C. Fourteen (9.5%) of the147 respondents reported on question 5c that they had purchased online pharmaceuticals, and three (21.4%) online buyers, and 2.0% of total respondents stated that they considered the presence of a stated privacy policy to be an important factor before deciding whether to purchase from the firm.

Table 3 indicates whether convenience of placing orders was deemed important to online pharmacy consumers. Eight (57.1%) online buyers of question 5c, (5.4% of total respondents) considered convenience an important factor when placing an online order for Canadian pharmaceuticals.

Table 2. Frequency of Considering Privacy Policy for Online Purchases

		Privacy Policy		
Online		Yes	No	Total
Yes	Count	3	11	14
	% within online	21.4%	78.6%	100.0%
	% within q5b (privacy)	100.0%	7.6%	9.5%
	% of total	2.0%	7.5	9.5
No	Count	0	133	133
	% within online	0.0%	100.0%	100.0%
	% within q5b (privacy)	0.0%	92.4%	90.5%
	% of total	0.0%	90.5%	90.5%
Total	Count	3	144	147
	% of total	2.0%	98.0%	100.0%

Table 3. Frequency of Considering Convenience for Online Purchases

		Convenience		
Online		Yes	No	Total
Yes	Count	8	6	14
	% within online	57.1%	42.9%	100.0%
	% within q5c (convenience)	100.0%	4.3%	9.5%
	% of total	5.4%	4.1%	9.5%
No	Count	0	133	133
	% within online	0.0%	100.0%	100.0%
	% within q5c (convenience)	0.0%	95.7%	90.5%
	% of total	0.0%	90.5%	90.5%
Total	Count	8	139	147
	% of total	5.4%	94.6%	100.0%

Table 4 shows 14 (9.5%) of the 147 respondents reported on question 5e regarding the importance of availability when deciding to purchase. Three (21.4%) of the online buyers (2.0% of all respondents) considered drug availability an important issue.

Consumers taking the survey may have found “other” reasons for considering whether to purchase from a Canadian online pharmacy (shown in Table 5). A majority of those who made an online purchase within the past year (n=10, 71.4%) considered other issues. This was 6.8% of the total respondents.

Table 4. Frequency of Considering Availability for Online Purchases

		Availability		
Online		Yes	No	Total
Yes	Count	3	11	14
	% within online	21.4%	78.6%	100.0%
	% within q5d (availability)	100.0%	7.6%	9.5%
	% of total	2.0%	7.5	9.5
No	Count	0	133	133
	% within online	0.0%	100.0%	100.0%
	% within q5d (availability)	0.0%	92.4%	90.5%
	% of total	0.0%	90.5%	90.5%
Total	Count	3	144	147
	% of total	2.0%	98.0%	100.0%

Table 5. Frequency of Considering Other Reasons for Online Purchases

		Other		
Online		Yes	No	Total
Yes	Count	10	4	14
	% within online	71.4%	28.6%	100.0%
	% within q5e (other)	100.0%	2.9%	9.5%
	% of total	6.8%	2.7%	9.5%
No	Count	0	133	133
	% within online	0.0%	100.0%	100.0%
	% within q5e (other)	0.0%	95.7%	90.5%
	% of total	0.0%	90.5%	90.5%
Total	Count	10	137	147
	% of total	6.8%	93.2%	100.0%

Table 6 outlines the findings for respondents' views on legal issues raised when using a Canadian online pharmacy. Of the 133 total respondents who did not use a Canadian pharmacy, a majority of respondents (n=68, 51.1%) revealed legal concerns kept them from making online pharmacy purchases. One respondent who made a pharmacy purchase within the past 12 months also answered this question expressing a concern about legal problems.

Table 6. Frequency of Considering Legal Issues for Online Purchases

		Legal		
Online		Yes	No	Total
Yes	Count	1	13	14
	% within online	7.1%	92.9%	100.0%
	% within q6a (legal)	1.4%	16.7%	9.5%
	% of total	0.7%	8.8%	9.5%
No	Count	68	65	133
	% within online	51.1%	48.9%	100.0%
	% within q6a (legal)	98.6%	83.3%	90.5%
	% of total	46.3%	44.2%	90.5%
Total	Count	69	78	147
	% of total	46.9%	53.1%	100.0%

The findings in Table 7 indicate whether lack of trust of online commerce was a factor that inhibited survey respondents from making an online pharmacy purchase. Few of the respondents (n=19, 14.3%) who did not make an online purchase found trust to be an overriding factor.

Table 7. Frequency of Considering Trust for Online Purchases

		Trust		
Online		Yes	No	Total
Yes	Count	0	14	14
	% within online	0.0%	100.0%	100.0%
	% within q6b (trust)	0.0%	10.9%	9.5%
	% of total	0.0%	9.5 %	9.5%
No	Count	19	114	133
	% within online	14.3%	85.7%	100.0%
	% within q6b (trust)	100.0%	89.1%	90.5%
	% of total	12.9%	77.6%	90.5%
Total	Count	19	128	147
	% of total	12.9%	77.6%	100.0%

Table 8 indicates the importance consumers place on the privacy of their personal medical data on a site, and whether their concerns prevented them from making online pharmacy purchases. Approximately one-third (37.6%) of 133 respondents reported on question 6c that they considered privacy issues a reason for not shopping online.

Table 8. Frequency of Considering Privacy for Online Purchases

		Privacy		
Online		Yes	No	Total
Yes	Count	0	14	14
	% within online	0.0%	100.0%	100.0%
	% within q6c (privacy)	0.0%	14.4%	9.5%
	% of total	0.0%	9.5 %	9.5%
No	Count	50	83	133
	% within online	37.6%	62.4%	100.0%
	% within q6c (privacy)	100.0%	85.6%	90.5%
	% of total	34.0%	56.5%	90.5%
Total	Count	50	97	147
	% of total	34.0%	56.5%	100.0%

Table 9. Frequency of Considering Quality for Online Purchases

		Quality		
Online		Yes	No	Total
Yes	Count	0	14	14
	% within online	0.0%	100.0%	100.0%
	% within q6d (quality)	0.0%	13.2%	9.5%
	% of total	0.0%	9.5 %	9.5%
No	Count	41	92	133
	% within online	30.8%	69.2%	100.0%
	% within q6d (quality)	100.0%	86.8%	90.5%
	% of total	27.9%	62.6%	90.5%
Total	Count	41	106	147
	% of total	27.9%	62.6%	100.0%

Table 9 outlines the findings for respondents' views on the quality of drugs when deciding to use online Canadian pharmacies. Approximately one-third (n=41, 30.8%) of survey respondents to this question held the view that the inability to guarantee the quality of drugs adversely affected their desire to complete online purchases from Canadian pharmacy Web sites.

Table 10. Frequency of Considering Other Factors for Online Purchases

		Other		
Online		Yes	No	Total
Yes	Count	3	11	14
	% within online	21.4%	78.6%	100.0%
	% within q6e (other)	2.8%	28.2%	9.5%
	% of total	2.0%	7.5 %	9.5%
No	Count	105	28	133
	% within online	78.9%	21.1%	100.0%
	% within q6e (other)	97.2%	71.8%	90.5%
	% of total	71.4%	19.0%	90.5%
Total	Count	108	39	147
	% of total	73.5%	26.5%	100.0%

Consumers taking the survey may have found “other” reasons for not purchasing from a Canadian online pharmacy. Table 10 shows if “other” factors were an issue to consumers. A majority of those who did not make online purchases within the past year (n=105, 78.9%) consider other issues. In addition, three respondents (n= 21.4%) of the 14 consumers who did make an online purchase also answered this question.

For survey respondents using a pharmacy "cost saving" (10 respondents within Table 1) and “none of the above” (10 respondents within Table 5) were the two main reasons given for making online purchases. For those consumers who had not used an online Canadian pharmacy in the past year, "legal issues" (68 respondents within Table 6) and “none of the above” (105 respondents within Table 10) were the most frequently noted explanations.

Consumer Purchasing Patterns and Viewpoints

This section provides a detailed analysis of consumer responses for each of the eight categories of information. Table 11 summarizes respondents’ views about the presence of privacy policies on the Canadian pharmacy Web sites listed in Appendix A,

as well as a site's use of privacy seal programs, such as BBBOnLine. Most respondents (n=84, 56.8%) agreed (summation of the "disagree" and "strongly disagree" cells for this and subsequent calculations in this section) that an online pharmacy should provide a link to their privacy policy on their home page. Likewise, 66.2% (n=98) of the participants responded negatively to Web sites whose privacy policies were not available via their home pages or that did not make their privacy policies available (n = 96, 64.9%). In addition, half of the respondents believe that a privacy seal program increased their trust in the Web site, while only 22.3% (n=23) disagreed. This last point was verified by Pennington, who indicates that privacy seals enhance trust in Internet sites (Pennington et al., 2003).

Table 11. Consumer Survey - Overall Privacy Findings

	Strongly Agree		Agree		Neither		Disagree		Strongly Disagree		NA	
Site Characteristic	n	%	n	%	n	%	n	%	n	%	n	%
Link on home page	25	16.9	59	39.9	44	29.7	18	12.2	0	0	1	0.6
No link on home Page	1	0.6	1	0.6	45	30.4	74	50.0	24	16.2	1	0.6
No posted policy	0	0.0	4	2.7	45	30.4	74	50.0	22	14.9	1	0.6
Use Seal	29	16.9	45	30.4	37	25.0	27	18.2	6	4.1	3	2.0

Table 12 shows the statistical findings on consumers' views regarding licensing and collection of prescription and health information. Respondents placed a high value on a pharmacy possessing a valid license (n=111,75%,), as well as being an actual pharmacy rather than a pharmacy intermediary (n=81, 54.8%,).

Pharmacy requirements for a consumer health profile and actual prescription script were slightly lower in consumer desirability. Most consumers either disagreed (n=48, 32.5%) with or felt neutral (n=50, 33.8%) about having to complete a required health profile. This may be due to the concerns of consumers when firms keep sensitive

data, such as health information. This was discussed by Choy et al. who indicates that trepidation about privacy makes online disclosure of medical information an especially sensitive issue to online consumers (Choy et al., 2001). This was also validated in the results of Table 8, showing that consumers placed a high priority in the privacy of their medical data, and would consider lack of privacy a reason for not shopping online.

Similarly, the majority of respondents either felt either neutral (n=42, 28.4%) or disagreed (n=50, 33.8%) with the requirement to provide an actual prescription for their prescription. However, over one-third (n=55, 37.2%) agreed with the prescription requirement, thus indicating a large deviation among consumer views on this issue.

Table 12. Consumer Survey - Licensing Findings

	Strongly Agree		Agree		Neither		Disagree		Strongly Disagree		NA	
Site Characteristic	n	%	n	%	n	%	n	%	n	%	n	%
License	38	25.7	73	49.3	30	20.2	6	4.1	0	0.0	1	0.6
Actual Pharmacy	30	20.3	51	34.5	51	34.5	15	10.1	0	0	1	0.6
Health profile	17	11.5	32	21.6	50	33.8	46	31.1	2	1.4	1	0.6
Prescription	17	11.5	38	25.7	42	28.4	43	29.1	7	4.7	0	0.0

Table 13 displays consumers' views related to collecting personal demographic information. Respondents indicated strong negative reactions across each of the five categories towards a site collecting personal information. More specifically, they disagreed with data collection of email addresses (n=78, 52.7%), mailing addresses (n=79, 53.4%), telephone numbers (n=80, 54%), credit card information (n= 86, 58.1%), and age and gender (n=66, 44.6%).

Table 13. Consumer Survey - Personal Demographic Findings

	Strongly Agree		Agree		Neither		Disagree		Strongly Disagree		NA	
Site Characteristic	n	%	n	%	n	%	n	%	n	%	n	%
Email	2	1.4	19	12.8	46	31.1	61	41.2	17	11.5	1	0.6
Mail address	2	1.4	20	13.5	44	31.1	59	39.9	20	13.5	1	0.6
Telephone	2	1.4	20	13.5	43	29.1	61	41.2	19	12.8	1	0.6
Credit card	2	1.4	16	10.8	41	27.7	55	37.2	31	20.9	1	0.6
Demographic	3	2.0	15	10.1	61	41.2	45	30.4	21	14.2	1	0.6

Computer hardware, software and cookie tracking results are compiled in Table 14. The findings illustrate consumers' strong propensity to disagree with the use of cookies and other software and hardware tracking. A small minority of respondents (n=16, 10.8%) agreed with cookie usage, while most disagreed with cookie tracking (n=79, 53.3%) and computer tracking (n=81, 54.8%). However, there were also a sizable number of respondents who were neutral towards using cookies (n=49, 33.1%) and usage tracking (n=49, 33.1%).

Table 14. Consumer Survey - Hardware/Software and Cookie Findings

	Strongly Agree		Agree		Neither		Disagree		Strongly Disagree		NA	
Site Characteristic	n	%	n	%	n	%	n	%	N	%	n	%
Uses cookies	3	2.0	13	8.8	49	33.1	60	40.5	19	12.8	2	1.4
IP address	3	2.0	12	8.1	50	33.8	57	38.5	23	15.5	1	0.6
Usage track	3	2.0	12	8.1	49	33.1	55	37.2	26	17.6	1	0.6
Domain name	3	2.0	13	8.8	47	31.8	58	39.2	24	16.2	2	1.4

The ability to modify or delete consumer information, along with opt-in and opt-out capability, showed to be desirable for most respondents (Table 15). Over half (n=88, 59.4%) of the respondents agreed that the ability to opt-out was a positive characteristic, as well as the opt-in characteristic (n=91, 61.4%). These results are validated by outside researchers, such as Adkinson et al. (2002) who indicated that Web users show a marked preference for opt-in policies. A similar number of respondents found it important to be

able to delete consumer information (n=88, 59.5%) as well as amend their personal data (n=87, 58.8%).

Table 15. Consumer Survey - Opt-In and Alteration Findings

	Strongly Agree		Agree		Neither		Disagree		Strongly Disagree		NA	
Site Characteristic	n	%	n	%	n	%	n	%	n	%	n	%
Can delete	26	17.6	62	41.9	53	35.8	6	4.1	0	0.0	1	0.6
Can alter	26	17.6	61	41.2	50	33.7	7	4.7	1	0.6	1	0.6
Opt-out	31	20.9	57	38.5	50	33.7	6	4.1	0	0.0	2	1.4
Opt-in	31	20.9	60	40.5	48	32.4	4	2.7	1	0.6	2	1.4

Table 16 outlines the findings for respondents' views on information disclosure to third parties and affiliate firms. A positive view was held of pharmacies that do not disclose consumer information, with 75.7% (n=112) of respondents agreeing that not disclosing information is indicative of a pharmacy's trustworthiness. Likewise, respondents revealed negative opinions (85.1%, n=126) about pharmacies that disclose consumer information to third-party firms, while 79.7% (n=118) disagreed with disclosing information to affiliates.

A smaller percentage of respondents expressed strong views towards pharmacies that disclose information when legally required, or if the consumers gave prior consent for disclosure. For pharmacies that must legally disclose information, the majority of respondents (n=70, 47.3%) held a neutral view. Over 40% (n=60) of respondents had a neutral view regarding consumer disclosure upon consent to release information, while 30.4% (n=53) agreed the practice is acceptable.

Table 16. Consumer Survey - Disclosure Findings

	Strongly Agree		Agree		Neither		Disagree		Strongly Disagree		NA	
Site Characteristic	n	%	n	%	n	%	n	%	n	%	n	%
Does not disclose	51	34.5	61	41.2	41	20.9	2	1.4	1	0.6	0	0.0
Does disclose	1	0.6	0	0.0	18	12.2	65	43.9	61	41.2	1	0.6
Consent to release	8	5.4	45	30.4	60	40.5	29	19.6	3	2.0	1	0.6
Perform services	2	1.4	13	8.8	58	39.2	57	38.5	14	9.5	0	0.0
Legally required	4	2.7	25	16.9	70	47.3	41	27.7	5	3.8	1	0.6
Acquired	1	0.6	2	1.4	61	41.2	66	44.6	15	10.1	1	0.6
Affiliates	1	0.6	0	0.0	26	17.6	66	44.6	52	35.1	1	0.6
Absolve URL	1	0.6	2	1.4	23	15.5	64	43.2	52	35.1	1	0.6
Third parties	1	0.6	0	0.0	21	14.2	62	41.9	59	39.9	2	1.4

Table 17. Consumer Survey - Security Findings

	Strongly Agree		Agree		Neither		Disagree		Strongly Disagree		NA	
Site Characteristic	n	%	n	%	n	%	n	%	n	%	n	%
SSL	26	17.6	58	39.2	45	30.4	14	9.5	1	0.6	2	1.4
Employees	29	19.6	56	37.8	41	27.7	14	9.5	2	1.4	2	1.4
Password	32	21.6	51	37.8	40	27.0	16	10.8	1	0.6	2	1.4
Firewall	27	18.2	55	37.2	42	28.4	15	10.1	1	0.6	2	1.4
Physical protection	32	21.6	53	35.8	40	27.0	14	9.5	1	0.6	2	1.4

The data in Table 17 show that respondents placed a high value on privacy policies that feature security characteristics. Over half (n=84, 56.8%) found favor with pharmacies whose privacy policy stated they offer Secure Sockets Layer (SSL) security on their Web site. The majority of respondents (n=85, 57.4%) also favored pharmacies who restricted their employees' access to confidential information, while 56.1% (n=83) approved of password protection, 55.4% (n=82) with firewall protection, and 57.4% (n=85) endorsed the practice of maintaining data in a secure environment. Interestingly, a few respondents disagreed with pharmacies posting information about their security characteristics in their privacy policies. The number of negative respondents ranged from a low of 15 respondents (10.1%) for physical protection to a high of 17 respondents (11.4%) for password protection.

Table 18. Consumer Survey - Miscellaneous Information Findings

	Strongly Agree		Agree		Neither		Disagree		Strongly Disagree		NA	
Site Characteristic	n	%	N	%	n	%	n	%	n	%	n	%
COPPA	12	8.1	18	12.2	56	37.8	47	31.8	4	2.7	3	2.0
Post changes	12	8.1	20	13.5	61	41.2	43	29.1	3	2.0	1	0.6
Email / phone	13	8.8	45	30.4	44	29.7	36	24.3	1	0.6	0	0.6

Table 18 illustrates the findings for several miscellaneous privacy policy characteristics. First, most respondents either had a neutral view (n=56, 37.8%) or disagreed (n=47, 31.8%) that posting a COPPA policy is advantageous. Only 21.6% (n=32) of respondents were in favor of a pharmacy stating that changes are posted to their privacy policy. A wide divergence of views existed on whether a pharmacy should post an email or telephone contact on their privacy policy page. Specifically, over one-third (39.2%) of respondents agreed, 29.7% were neutral, and 24.9% disagreed.

Pharmacy Web Site Analysis and Findings

The number of Canadian pharmacies that display privacy policies within their Web sites is illustrated in Table 19. The majority of sites placed the link on their home page (n=16, 64.0%), while 22% (n=3) placed a privacy link elsewhere on their site. Three sites did not contain a privacy policy link. One consequence of this practice is to create a hardship for site users, who may overlook a privacy policy where the link is not posted on the home page. Because the majority of sites do post privacy policies on their pages, this could result in a positive impact to online consumers' views of the sites. As indicated in Table 11, most survey respondents maintained that online pharmacies should provide privacy policy links on their home page, and responded negatively to sites that did not post policies.

Table 19. Pharmacy Review - Overall Privacy Findings

	Yes		No	
Site Characteristics	n	%	n	%
Privacy link on home page	16	64.0	9	36.0
Privacy link on non-home page	3	22.0	22	88.0
No privacy policy	3	22.0	22	88.0

Table 20 shows seven pharmacies (28%) indicated membership with the Canadian International Pharmacy Association (CIPA). None indicated participation in the Verified Internet Pharmacy Practice Sites (VIPPS), a division of the National Association of Boards of Pharmacy. Marketing research studies by Pennington et al. (2003) reveal that displaying privacy seals, such a BBBOnLine or TRUSTe, has a positive impact on consumers' views of online sites. This view corresponds to the results in this study shown in Table 11, where most respondents felt that a privacy seal program was beneficial. However, despite these research findings, most of the 25 online pharmacies surveyed did not use this valuable tool.

Table 20. Pharmacy Review - Privacy Seal Findings

	Yes		No	
Site Characteristics	n	%	n	%
BBBonline	3	12.0	22	88.0
TRUSTe	1	4.0	24	96.0
CIPA	7	28.0	18	72.0
VIPPS	0	0.0	25	100.0

The results of Table 12 show a large number of respondents are concerned about the online pharmacy holding a valid pharmacy license. Seventy-five percent of consumers felt that a licensed pharmacy was valuable, and 54% felt it was important to be an actual pharmacy instead of an intermediary. Contrary to consumers' desires, not all pharmacies are licensed, or if they are, they may not specify this designation on their site. In a study of Canadian online pharmacies, PharmacyChecker.com (2003b) estimated that 50% of sites do not hold valid Canadian pharmacy licenses. Table 21 illustrates that 68%

(n=17) of pharmacies in this study display ownership of a license on their Web site. Forty-four percent of the Web sites (n=11) indicated they are actual pharmacies as opposed to intermediaries.

Table 21. Pharmacy Review - Licensing Findings

	Yes		No	
Site Characteristics	n	%	n	%
License number on site	17	68.0	8	32.0
Actual pharmacy	11	44.0	14	56.0
Prescription through affiliate	14	56.0	18	44.0

As can be seen in Table 22, 96% (n=24) of the pharmacies in this study indicated in their privacy policies that they require a completed health profile and an original prescription (or copy) in order to purchase prescriptions on their Web site.

Table 22. Pharmacy Review - Medical Information Findings

	Yes		No	
Site Characteristics	n	%	n	%
Health profile	24	96.0	1	4.0
Requires prescription	24	96.0	1	4.0

Table 23 exhibits the pharmacies whose privacy policies designate the specific types of personal and demographic information they collect. Approximately one-third of pharmacies (28% - 36%) revealed they collect some information, such as the customer's email, address, telephone number, credit card information, and demographics (i.e., age, gender). The pharmacies did not show a propensity to request consumers' social security numbers. Web site collection of personal data on Canadian pharmacies contradicts consumers views compiled in Table 13. Survey takers had negative reactions to firms collecting personal data, yet privacy policies results in Table 23 show firms continue to collect this information.

Table 23. Pharmacy Review - Demographic Information Findings

	Yes		No	
Site Characteristics	n	%	n	%
Email	8	32.0	17	68.0
Social security	0	0.0	25	100.0
Address	9	36.0	16	64.0
Telephone	9	36.0	16	64.0
Credit card	9	36.0	16	64.0
Demographics	7	28.0	18	72.0

Table 24 illustrates that few of the Canadian online pharmacies (n=8, 32.0%) explicitly mention that they use cookies. Nine of the privacy policies reviewed in this study indicated the use of third-party cookies. Consumer attitudes found in Table 14 show that most respondents (n=79, 52.8%) disagreed with cookie tracking, so the collection results showing minimal cookie usage in Table 24 may indicate consumers would view these online Canadian pharmacies in a more positive light.

Table 24. Pharmacy Review - Cookies Findings

	Yes		No	
Site Characteristics	n	%	n	%
Use cookies	8	32.0	17	68.0
Third party cookies	9	36.0	16	64

Table 25 shows that few online pharmacies in this research study posted statements revealing they collect information through tracking. Six pharmacies (24.0%) mentioned that they collect IP addresses and use consumer hardware information to track consumer usage patterns. Only 8.0% (n=2) confirmed they collect information on browser types and domain names, while 4.0% (n=1) admit to collecting data on referring Web site addresses and log files.

Table 25. Pharmacy Review - Hardware/Software Tracking Findings

	Yes		No	
Site Characteristics	n	%	n	%
IP address	6	24.0	19	76.0
Browser types	2	8.0	23	92.0
Refer Web site address	1	4.0	24	96.0
Log file	1	4.0	24	96.0
Usage tracking	6	24.0	19	76.0
Domain name	2	8.0	23	92.0

An interesting result, shown in Table 26, is that few online pharmacies mention their opt-in or opt-out policies. None showed that they subscribe to opt-in guidelines and 21 (84.0%) mentioned opt-out options. This result validates Cadogan's (2001) research that explains most online merchants prefer to use opt-out strategies as opposed to opt-in.

Table 26. Pharmacy Review - Opt-in / Opt-out Findings

	Yes		No	
Site Characteristics	n	%	n	%
Opt-in	0	0.0	25	100.0
Opt-out	21	84.0	4	16.0

Table 27. Pharmacy Review - Ability to Update Data Findings

	Yes		No	
Site Characteristics	n	%	n	%
Delete information	2	8.0	23	92.0
Delete from archive	0	0.0	25	100.0
Update/amend data	10	40.0	15	60.0

Few pharmacy Web sites denote that they allow customers to *delete* information from their databases (n=2, 8.0%) or their archived backup databases (n=0, 0%). A higher percentage of Web sites (n=10, 40.0%) display policies that inform consumers they can *update* or *amend* their personal information (Table 27). Yet, consumer preference in Table 15 indicates that the ability to delete or alter information is important to consumers, with 59.5% relating it is important to be able to delete information and 58.8% finding it important to amend personal data.

Table 28. Pharmacy Review - Disclosure Findings

	Yes		No	
Site Characteristics	n	%	n	%
Does not share with third party	12	48.0	13	52.0
Discloses data to third party	2	8.0	23	92.0
Discloses if consent	6	24.0	19	76.0
Discloses if performing services	7	28.0	18	72.0
Legally required	11	44.0	14	56.0
Merger	8	32.0	17	68.0
Disclose to affiliates	6	24.0	19	76.0

Table 28 shows that approximately half (n=12, 48.0%) of the pharmacies surveyed in this study have privacy policies that specify they do not share information with third parties. Only 8.0% (n=2) post that they disclose information to third-party firms, 24.0% (n=6) disclose information if the consumer consents, 28.0% (n=7) disclose data if performing services, 44.0% (n=11) if legally required, 32.0% (n=8) if the firm merges, and 24.0% (n=6) denote they release data to affiliates.

Table 29. Pharmacy Review - Security Findings

	Yes		No	
Site Characteristics	n	%	n	%
SSL	6	24.0	19	76.0
Restrict employee access	5	20.0	20	80.0
Passwords	3	12.0	22	88.0
Third-party credit card process	0	0.0	25	100.0
Firewalls	3	12.0	22	88.0
Physical protection	5	20.0	20	80.0

Security issues compiled in Table 17 show respondents place a high value on information security. Yet, the statistics of online firms who post comprehensive security policies on their privacy site does not correspond to consumers' desires. Table 29 shows that a minority of the pharmacies display information about the security characteristics of their Web sites. Findings range from a high number (24.0%, n=6) of pharmacies who post information about their use of SSL security to a low number (0.0%, n=0) of pharmacies who reveal their use of third-parties to process credit card data.

Table 30. Pharmacy Review - Absolve Collection Findings

	Yes		No	
Site Characteristics	n	%	n	%
Absolves outside links	3	12.0	22	88.0
Absolves data collection	4	16.0	21	84.0

The findings in Table 30 indicate whether or not online pharmacies exempt themselves from legal issues resulting from third-parties collecting data from their Web sites. Few of the pharmacies discharge liability third-party firms or links from third-party Web sites. Only 12.0% (n=3) of pharmacies absolve themselves when outside online firms link to their Web site, and 16.0% (n=4) release themselves from issues related to data collected by third parties.

A variety of miscellaneous findings are reviewed in Table 31. None of the online pharmacies surveyed post information about the legal requirements of the Children's Online Privacy Protection Act (COPPA). Over half of the pharmacies (n=13, 52%) have posted an email or phone contact on their privacy policy page, and 40.0% (n=10) state that they post updates to the privacy policy when changes occur.

Table 31. Pharmacy Review - Miscellaneous Findings

	Yes		No	
Site Characteristics	n	%	n	%
COPPA	0	0.0	25	100.0
Changes to policy	10	40.0	15	60.0
Email or phone contact	13	52.0	12	48.0

The comprehensiveness of the online pharmacies' privacy policies was determined by investigating 49 possible characteristics. Table 32 shows the total number of characteristics compiled for each of the pharmacies. None of the pharmacies' privacy policies included all possible characteristics. The top three pharmacies that contained the majority of options were: (a) Mediplan Health (n=30), (b) PeopleRx (n=29), and (c)

Canada Drugs (n=23). The Web sites with the least comprehensive privacy policies include: (a) Best Canadian Pharmacy (n=3), (b) DirectDrugmart (n=4), (c) Meds 4 Less (n=4), and (d) SuperSaveRx (n=4). It is interesting to note that the last three aforementioned pharmacies do not have a privacy policy on their Web site; however, each requires consumers to provide medical history and prescriptions.

Table 32. Pharmacy Review - Number of Characteristics per Pharmacy

Pharmacy	Number
Abconlinepharmacy.com	7
Best Canadian Pharmacy	3
Canada Drugs	23
Canada Online Healthlink	7
Canadian Med Service	17
Canadian Pharmacy Network	22
Canadian Prescription Savers	5
CanadianMeds.com	19
CrossBorderPharmacy.com	18
DirectDrugmart	4
Discount Canadian Prescriptions	9
Discount Rx Mart	5
Doctorsolve Healthcare	14
MedCenter Canada	5
Mediplan Health	30
Meds 4 Less	4
Medsforall.com	6
PeopleRx	29
Rxbyfax	5
RxCounter.com	19
Smart Med Pharmacy	7
SuperSaveRx	4
The Canadian Drugstore	7
United Prescription Service	21
Universal Drugstore	22

Summary of Results

This chapter reviewed the findings of an in-depth analysis of the privacy policies and procedures of 25 major online Canadian pharmacies, as well as the purchasing patterns and viewpoints of 147 consumers. The data has been presented in textual form and supported with tabulated data.

The vast majority of 147 survey respondents strongly agreed or agreed that privacy policy factors were important reasons when considering whether to use online Canadian pharmacy Web sites. These characteristics included displays of privacy policies on the site, licensing, security, opt-in ability, seal programs, and other factors. Some of the characteristics garnered more weight than others, but overall the inclusion of most privacy factors was important to consumers. However, consumer desire for privacy was sometimes mitigated by other concerns, such as cost and legal issues.

Consumers' desires for comprehensive privacy factors on Canadian sites did not correlate to actual practices of 25 major online Canadian pharmacies. For example, the ability to modify or delete consumer information, along with opt-in and opt-out capability, was desired by most respondents. However, few of the pharmacy Web sites in this study indicate that they allow customers to delete information from their databases or their archived backup databases; however, a higher percentage of Web sites display policies that inform consumers they can update or amend their personal information. The analysis shows an incongruity between consumers' desires for privacy factors on Canadian Web sites versus the actual privacy practices of these pharmacy sites. The results of this study leads to the next chapter, which contains the conclusion, implications and recommendations for future research on this subject.

Chapter 5

Conclusions, Implications, Recommendations and Summary

This chapter discusses the outcomes of the research, discusses implications of the findings, and presents recommendations regarding how this research can advance knowledge relating to the issues of consumer privacy in the online arena, especially related to Canadian online pharmacies. A summary concludes the chapter.

Conclusions

The four goals and research questions of this study were met. These included the following:

1. What types of privacy issues do Canadian online pharmacies address?
2. Do gaps exist in privacy protection provided to consumers of online Canadian pharmacies?
3. Which online pharmacies offer the most comprehensive privacy policies and what are their strengths and weaknesses?
4. What privacy and non-privacy criteria do consumers use when deciding to order from these sites, and what factors do non-buyers cite for not purchasing drugs?

The first goal was to identify the types of privacy issues being addressed by Canadian online pharmacies' policies. To answer this question, a framework of analysis was used to compile privacy issue characteristics. The literature review, prior research studies, and best-practices of the online pharmacy industry helped in the compilation of

privacy characteristics to be included in both the online user survey and the review of 25 online pharmacies.

A second goal of this study was to determine the gaps in privacy protection for consumers of online pharmacies. Results showed that most Canadian online pharmacies do incorporate some measure of privacy policies into their Web sites; however, the survey of 25 of these sites showed that most sites did not adhere to best-practices guidelines for effective privacy policies. Further, some sites were found to be more stringent and comprehensive in their policies than others. The Research Question 2 was answered by showing that there are significant gaps in privacy protection for consumers among these types of Web sites.

The third research goal was to review which online pharmacies are the most effective (defined in chapter one as addressing a variety of privacy policies), and to analyze their strengths and weaknesses. Mediplan Health, PeopleRx and Canada Drugs were found to have the most comprehensive privacy policies. The results of the consumer survey confirmed that online pharmacies with the most effective privacy policies were those that assured their customers and potential customers that they had adequate security features in place and that consumers and potential consumers would be provided with the opportunity to revise, change, or otherwise alter their information if they required or desired to do so, as well as opt-out. Clearly, the criteria consumers use when deciding to order from these sites include wanting some control over how their personal information would be used, and who would have access to it in the future.

The fourth goal of the study was to determine the criteria consumers used when deciding whether to order from a site, what privacy issues were important to them, and

what reasons were given by non-users for not utilizing the sites. This portion of the study involved an online survey of consumers who utilize medical Web sites, and therefore were more likely to use online pharmacies for their pharmaceutical purchases. A percentage of medical Web site users had used Canadian pharmacies and contributed first-hand knowledge of their views and concerns about using online pharmacy sites. Because many Americans use online Canadian pharmacies to take advantage of the lower cost of prescription drugs, it was conceivable that the research would indicate that although these consumers are worried about their privacy, they would prove to be more concerned with the price and availability of the products. The results of the online survey showed that online consumers are concerned with privacy issues, although some privacy policy characteristics, such as security and ability to opt-out, are more highly valued than others, such as COPPA warnings. Those consumers who did not use a Canadian online pharmacy also indicated that privacy was important; however, certain guidelines related to privacy were found to be more important than others.

While the consumer survey showed respondents had a positive view towards comprehensive privacy policies, when consumers were faced with the choice between purchasing lower-cost pharmaceuticals or choosing a site with strong privacy policy guidelines, they often placed higher value on low cost. This is consistent with existing research showing that consumers recognize the trade-offs between privacy and economic benefits they enjoy with online purchasing (U.S. Federal Trade Commission, 2004).

Another important conclusion related to the question of how many sites adhere to their own policies, and which aspects of privacy issues are included on a privacy page. One of the guiding tenets of this study was that an online pharmacy site that scored well

on the statistics gathered in the study could be regarded as being highly effective in promoting customer privacy and adhering to privacy laws and guidelines. The results of the survey of the 25 online Canadian pharmacies showed that most of the sites provided a privacy link on their home page, most required a health profile and an original or copy of a prescription, and a majority featured their license number on their site. However, beyond these commonalities, there existed vast differences in the manner in which these services were administered and the security and privacy provisions that were used. This lack of policy consistency can result in consumer confusion about drug information, and the potential for third-party providers to obtain sensitive information about the consumers.

Implications

This study has implications for online consumers as well as Canadian pharmacies and their customers. The primary benefit for consumers is a methodology for reviewing a variety of factors and best-practices related to online privacy practices. It is imperative to realize that because of the myriad of U.S. and Canadian laws, as well as self-regulation approaches to privacy, consumers may not have a thorough understanding of how their online privacy is protected and what features they should review in a comprehensive privacy policy. In addition, there is no overall Web site comparison of the privacy policies for online Canadian pharmacies. Although this study is not meant to be a study of all sites, its results provide an understanding of best-practice policy features that consumers can review on e-commerce sites, and affords a review of 25 major Canadian pharmacy sites.

Using online pharmacy firms involves both risks as well as the benefits that online shopping can bring to bear on modern healthcare practices. Unfortunately, the research showed that, in some cases, online pharmacies operate outside of accepted pharmaceutical and best-practice privacy practice guidelines. Notwithstanding the dangers typically associated with these online pharmacy providers, the high costs of prescription medications in the United States has compelled many consumers to seek alternatives through these online outlets.

Therefore, it is clear that consumers should be cautious of online pharmacies as a means of obtaining products as well as cautious of practices online that are illegal in an offline environment. For instance, in some cases, online pharmacies only require customers to complete a modest questionnaire before ordering prescription drugs. Although this reduces the amount of private information held by the site, it also bypasses any personal evaluation by a healthcare professional, a situation that may be detrimental to the consumer's health. Following the recommendations of Cadogan (2001), consumers need comprehensive and accurate information to protect their privacy; it is recommended that consumers familiarize themselves with both the security and privacy issues involved in such online transactions, and investigate a potential online pharmacy by checking the online sites for privacy policy guidelines or any potential consumer feedback.

In addition to implications for consumers, the study has consequences for Web pharmacies and offers practical applications for their improvement. If these firms choose to implement stricter privacy polices than those used currently, they can develop their overall policy based on best-practice elements contained in this study. This model may be

helpful for those pharmacies seeking to capture additional market share among U.S. consumers who place a value on more comprehensive privacy concerns.

A heightened awareness of consumers' attitudes toward privacy could serve as a means for pharmacies to develop more comprehensive privacy pages based on consumers' attitudes and desires. The opportunity for firms to evaluate which privacy features are most important to their shoppers will allow them to tailor their online privacy policies. For example, an online firm can use the methodology and survey instruments developed in this paper to analyze the behaviors and desires of its own customers. If its customers have an overriding desire for tighter privacy controls, it may be advantageous for the site to incorporate the best-practice privacy features described in this study. Alternatively, if a firm discovers that the low cost of the pharmaceuticals overrides privacy concerns, it may make a business decision not to spend time being concerned about the nature of its privacy policy.

Recommendations

Because of the ever-changing information in Web sites, it is highly probable that the privacy features listed in the 25 reviewed Canadian pharmacy sites may become outdated with the passage of time. Thus, follow-up studies of these sites and a comparison of pre- and post- results would indicate the levels of privacy changes among sites, especially in relation to simultaneous modification to laws, regulations, and political changes.

Hundreds of Canadian mail-order pharmacies now exist on the Internet; this study was limited to 25 sites. It is recommended that analysis of other sites be undertaken, as

such studies may indicate whether the findings of this study are representative of other online pharmacies.

Further research also is needed in the area of consumer attitudes towards privacy policies among online Canadian pharmacies. This study was limited to 147 respondents who utilized at least one of several online medical Web sites. It is plausible that privacy priorities may be different among consumers who utilize other types of Web sites. Further research studies should involve surveying respondents who use other Web sites and whose demographic characteristics are representative of all users.

Results of this study showed considerable variation in the comprehensiveness of Canadian online pharmacy privacy policies. However, a statement of policy is not the same as effective implementation, nor is it necessarily the case that privacy policies, whether comprehensive or not, are effective in preventing the compromise of personal information. Thus, it is recommended that further research in the effectiveness of such policies needs to be undertaken, in the hope of determining whether more stringent policies result in fewer compromises of personal information.

Conclusion

Although most of the 25 Canadian online pharmacies examined in this study have some elements of a privacy policy, their level of comprehensiveness is inconsistent. In addition, it was found that although consumers value stringent and comprehensive policies, other factors, such as cost and availability, play a key role in determining whether consumers use a site. Such choices should not have to be made in an area as critical as needed medications. Canadian online pharmacy Web sites should provide a more consistent level of privacy protection than currently offered.

Appendix A

Canadian Online Pharmacies Chosen for Evaluation

Abconlinepharmacy.com	http://www.abconlinepharmacy.com
Best Canadian Pharmacy	http://www.best-canadian-pharmacy.com
Canada Drugs	http://www.canadadrugs.com
Canada Online Healthlink	http://www.candrugstore.com
Canadian Med Service	http://www.canadianmedservice.com
Canadian Pharmacy Network	http://www.canadianpharmacynetwork.com
Canadian Prescription Savers	http://www.canadianprescriptionsavers.com
CanadianMeds.com	http://www.canadianmeds.com
CrossBorderPharmacy.com	http://www.crossborderpharmacy.com
DirectDrugmart	http://www.directdrugmart.com
Discount Canadian Prescriptions	http://www.dcpdrugs.com
Discount Rx Mart	http://www.discountrxmart.com
Doctorsolve Healthcare	http://www.doctorsolve.com
MedCenter Canada	http://www.medcentercanada.com
Mediplan Health	http://www.rxnorth.com
Meds 4 Less	http://www.apromedica.com
Medsforall.com	http://www.medsforall.com
PeopleRx	http://www.peoplerx.com
Rxbyfax	http://www.rxbyfax.com
RxCounter.com	http://www.rx-counter.com

Smart Med Pharmacy	http://www.smartmed.ca
SuperSaveRx	http://www.supersaverx.com
The Canadian Drugstore	http://www.thecanadiandrugstore.com
United Prescription Service	http://www.smartchoicepharmacy.com
Universal Drugstore	http://www.universaldrugstore.com

Appendix B

Spreadsheet of Privacy Policy Information for Canadian Online Pharmacies

Table 33. Spreadsheet of Privacy Policy Information for Canadian Online Pharmacies

			ABC	Best	CanDrugs	Candrugst	Canmedsvc
General Info on Site	Overall privacy policy						
		privacy link on home page			x	x	x
		privacy link on non-home page	x	x			
		no privacy policy					
	Privacy seal use						
		BBBOnLine					x
		TRUSTe					
		CIPA seal	x		x		
		VIPPS					
	Licensing						
		License number on site	x		x		x
		Actual Pharmacy	x		x		x
		Offers prescriptions through affiliate		x		x	
	Medical information						
		requires health profile	x		x	x	x
		requires original or copy of prescription	x		x	x	x

Table 33. (Continued)

			ABC	Best	CanDrugs	Candrugst	Canmedsvc
Info contained within privacy policy							
	Demographic information						
		email			X		
		social security					
		address			X		
		telephone			X		
		credit card			X		
		demographics (gender, age)			X		
	Use of cookies						
		Uses cookies					X
		Third-party can place cookies					
	Computer software and hardware information collected from cookies						
		IP address					
		browser types					
		referring web site address					
		log files					
		usage tracking					
		domain name					
	Opt-in and opt-out						
		Opt-in ability					
		Opt-out ability					X
	Personal update of information in system						
		Can delete information					X

Table 33. (Continued)

		ABC	Best	CanDrugs	Candrugst	Canmedsvc
	Can delete from archived database					
	Can update / amend data in database			X		X
Disclosure of information to third parties and affiliates						
	does not share with third parties		X	X	X	X
	discloses data to third parties					
	if you consent			X		
	if required to perform services			X		X
	if legally required			X		X
	if company acquires firm or merges			X		X
	discloses data to affiliates	X		X		X
Steps to provide security						
	SSL and/or encryption				X	
	Only allow specific personnel access to data			X	X	
	Password login system					
	Credit cards handled by third party					
	Firewalls			X		

Table 33. (Continued)

			ABC	Best	CanDrugs	Candrugst	Canmedsvc
		Servers/data kept in protected environment			x		
	Absolving data collection						
		Absolves outside links					
		Absolves data collected by others					
	Does not collect data about children under 13						
	Will post changes to privacy policy				x		X
	Provides email or phone contact on privacy page				x		X
			Can pharmnet	Can prescr	Canmeds	Cross bord	Direct drug
General Info on Site	Overall privacy policy						
		privacy link on home page	x		x	X	
		privacy link on non-home page					
		no privacy policy		x			x
	Privacy seal use						
		BBBOnLine					
		TRUSTe					
		CIPA seal				X	
		VIPPS					

Table 33. (Continued)

			Can pharmnet	Can prescr	Canmeds	Cross bord	Direct drug
	Licensing						
		License number on site	x	x		X	
		Actual Pharmacy				X	
		Offers prescriptions through affiliate	x	x	x		x
	Medical information						
		requires health profile	x	x	x	X	x
		requires original or copy of prescription	x	x	x	X	x
Info contained within privacy policy							
	Demographic information						
		email	x		x	X	
		social security					
		address	x		x	X	
		telephone	x		x	X	
		credit card	x		x	X	
		demographics (gender, age)	x		x	X	
	Use of cookies						
		Uses cookies	x		x		
		Third-party can place cookies					

Table 33. (Continued)

		Can pharmnet	Can prescr	Canmeds	Cross bord	Direct drug
Computer software and hardware information collected from cookies						
	IP address	X		X		
	browser types					
	referring web site address					
	log files usage tracking	X		X		
	domain name	X				
Opt-in and opt-out						
	Opt-in ability					
	Opt-out ability					
Personal update of information in system						
	Can delete information					
	Can delete from archived database					
	Can update / amend data in database	X		X	X	
Disclosure of information to third parties and affiliates						
	does not share with third parties					
	discloses data to third parties if you consent				X	

Table 33. (Continued)

		Can pharmnet	Can prescr	Canmeds	Cross bord	Direct drug
	if required to perform services					
	if legally required	x		x	X	
	if company acquires firm or merges	x		x	X	
	discloses data to affiliates	x				
Steps to provide security						
	SSL and/or encryption					
	Only allow specific personnel access to data					
	Password login system					
	Credit cards handled by third party					
	Firewalls					
	Servers/data kept in protected environment					
Absolving data collection						
	Absolves outside links	x		x	X	
	Absolves data collected by others	x		x		
Does not collect data about children under 13		x		x	X	
Will post changes to privacy policy		x		x	X	
Provides email or phone contact on privacy page		x		x	X	

Table 33. (Continued)

			Dcpdrugs	Discrx	Doctorsolv	Med center	Rxnorth
General Info on Site	Overall privacy policy						
		privacy link on home page	x	x	x		x
		privacy link on non-home page					
		no privacy policy				x	
	Privacy seal use						
		BBBOnLine					x
		TRUSTe					
		CIPA seal			x		x
		VIPPS					
	Licensing						
		License number on site	x		x	x	x
		Actual Pharmacy	x				x
		Offers prescriptions through affiliate		x	x	x	
	Medical information						
		requires health profile	x	x	x	x	x
		requires original or copy of prescription	x	x	x	x	x
Info contained within privacy policy							
	Demographic information						
		email					x
		social security					

Table 33. (Continued)

		Dcpdrugs	Discrx	Doctorsolv	Med center	Rxnorth
	address			X		X
	telephone			X		X
	credit card			X		X
	demographics (gender, age)					X
Use of cookies						
	Uses cookies					X
	Third-party can place cookies					
Computer software and hardware information collected from cookies						
	IP address					X
	browser types					X
	referring web site address					X
	log files					
	usage tracking					X
	domain name					X
Opt-in and opt-out						
	Opt-in ability					
	Opt-out ability	X				X
Personal update of information in system						
	Can delete information					
	Can delete from archived database					
	Can update / amend data in database					X
Disclosure of information to third parties and affiliates						

Table 33. (Continued)

		Dcpdrugs	Discrx	Doctorsolv	Med center	Rxnorth
	does not share with third parties	X		X		X
	discloses data to third parties					
	if you consent					X
	if required to perform services			X		X
	if legally required			X		X
	if company acquires firm or merges					X
	discloses data to affiliates					X
Steps to provide security						
	SSL and/or encryption	X				X
	Only allow specific personnel access to data			X		
	Password login system					
	Credit cards handled by third party					
	Firewalls					
	Servers/data kept in protected environment					X
Absolving data collection						
	Absolves outside links					
	Absolves data collected by others		X			
Does not collect data about children under 13						

Table 33. (Continued)

			Dcpdrugs	Discrx	Doctorsolv	Med center	Rxnorth
	Will post changes to privacy policy						x
	Provides email or phone contact on privacy page		x		x		x
			Apromed	Meds forall	Peoplerx	Rxbyfax	Rx counter
General Info on Site	Overall privacy policy						
		privacy link on home page		x	x		x
		privacy link on non-home page					
		no privacy policy	x			x	
	Privacy seal use						
		BBBOnLine					
		TRUSTe			x		
		CIPA seal					
		VIPPS					
	Licensing						
		License number on site			x	x	x
		Actual Pharmacy				x	
		Offers prescriptions through affiliate	x	x	x		x
	Medical information						
		requires health profile	x	x	x	x	x
		requires original or copy of prescription	x	x	x	x	x
Info contained within privacy policy							

Table 33. (Continued)

		Apromed	Meds forall	Peoplerx	Rxbyfax	Rx counter
Demographic information						
	email social security			X		
	address			X		
	telephone			X		
	credit card			X		
	demographics (gender, age)			X		
Use of cookies						
	Uses cookies Third-party can place cookies			X		
Computer software and hardware information collected from cookies						
	IP address			X		X
	browser types referring web site address			X		
	log files			X		
	usage tracking			X		X
	domain name					
Opt-in and opt-out						
	Opt-in ability Opt-out ability					X
Personal update of information in system						
	Can delete information Can delete from archived database					X

Table 33. (Continued)

		Apromed	Meds forall	Peoplerx	Rxbyfax	Rx counter
	Can update / amend data in database			X		X
Disclosure of information to third parties and affiliates						
	does not share with third parties		X			
	discloses data to third parties			X		X
	if you consent		X	X		
	if required to perform services			X		X
	if legally required			X		X
	if company acquires firm or merges					X
	discloses data to affiliates			X		
Steps to provide security						
	SSL and/or encryption			X		X
	Only allow specific personnel access to data			X		
	Password login system			X		X
	Credit cards handled by third party					
	Firewalls			X		
	Servers/data kept in protected environment			X		X
Absolving data collection						
	Absolves outside links					

Table 33. (Continued)

			Apromed	Meds forall	Peoplerx	Rxbyfax	Rx counter
		Absolves data collected by others					
	Does not collect data about children under 13						
	Will post changes to privacy policy				x		x
	Provides email or phone contact on privacy page				x		x
			Smartmed	Super save	The Canada	Smart choice	Universal
General Info on Site	Overall privacy policy						
		privacy link on home page			x	x	X
		privacy link on non-home page	x				
		no privacy policy		x			
	Privacy seal use						
		BBBOnLine					X
		TRUSTe					
		CIPA seal				x	X
		VIPPS					
	Licensing						
		License number on site	x		x	x	X
		Actual Pharmacy	x	x		x	X
		Offers prescriptions through affiliate			x		
	Medical information						
		requires health profile	x	x	x	x	X

Table 33. (Continued)

			Smartmed	Super save	The Canada	Smart choice	Universal
		requires original or copy of prescription	x	x	x	x	X
Info contained within privacy policy							
	Demographic information						
		email social security				x	X
		address				x	X
		telephone				x	X
		credit card				x	X
		demographics (gender, age)					X
	Use of cookies						
		Uses cookies				x	
		Third-party can place cookies					
	Computer software and hardware information collected from cookies						
		IP address				x	
		browser types					
		referring web site address					
		log files					
		usage tracking				x	
		domain name					
	Opt-in and opt-out						
		Opt-in ability					
		Opt-out ability					

Table 33. (Continued)

		Smartmed	Super save	The Canada	Smart choice	Universal
Personal update of information in system						
	Can delete information					
	Can delete from archived database					
	Can update / amend data in database				x	X
Disclosure of information to third parties and affiliates						
	does not share with third parties	x		x	x	X
	discloses data to third parties					
	if you consent					X
	if required to perform services					X
	if legally required				x	X
	if company acquires firm or merges				x	
	discloses data to affiliates					
Steps to provide security						
	SSL and/or encryption			x		
	Only allow specific personnel access to data					X
	Password login system				x	
	Credit cards handled by third party					
	Firewalls					X

Table 33. (Continued)

		Smartmed	Super save	The Canada	Smart choice	Universal
	Servers/data kept in protected environment					X
Absolving data collection						
	Absolves outside links					
	Absolves data collected by others				x	
Does not collect data about children under 13						
Will post changes to privacy policy					x	X
Provides email or phone contact on privacy page		x			x	X

Appendix C

Online Survey Questions

This survey will be tabulated and analyzed by a research group to determine consumer's views of Canadian online pharmacies and to evaluate how their privacy policies can be used to better serve their purchasing needs.
*Please note-Your individual answers will be anonymous and completely confidential. It is your opinion that is important. Individual answers will not be available to anyone outside the research institution conducting this survey. Your answers will be combined with the answers from other respondents for a composite picture of consumer's attitudes towards Canadian online pharmacies and their privacy policies.
The survey consists of 45 questions and should take approximately 10-15 minutes to complete.

Demographics.

1. What is your gender?
   a. Male
   b. Female

2. What is your age?

   a. Under 40
   b. 41 – 60
   c. Over 60

3. Do you have a prescription insurance plan that pays for some or all of your prescriptions?

   a. Yes
   b. No

4. Have you used an online Canadian Pharmacy to order your prescriptions within the past year?

   a. Yes
   b. No

5. If you have used an online Canadian pharmacy within the past year, what were the main reasons you chose to use it? Please choose all that apply

   a. Cost savings
   b. Privacy policy on site

c. Convenience
d. Availability of products
e. Other/None of the above

6. If you have not used an online Canadian pharmacy within the past year, what were the main reasons you chose not to use it? Please check all that apply

a. Legal issues with importing drugs from Canada
b. Don't trust online purchasing
c. Concerned about privacy and personal medical data
d. Concerned about the quality of drugs from Canada
e. Other/None of the above

Overall Privacy. (on a scale from 1 to 5)

7. I am more likely to use an online Canadian pharmacy if a link to the privacy policy is somewhere on the home page.
8. I am more likely to use an online Canadian pharmacy if there is not a link to the privacy policy somewhere on the home page.
9. I am likely to use an online Canadian pharmacy if there is not a posted privacy policy.
10. I am likely to use an online Canadian pharmacy if the site uses a privacy seal (such as Better Business Bureau Online).

Consumer/Licensing. (on a scale from 1 to 5)

11. I am more likely to use an online Canadian pharmacy if there is a pharmacy license prominently displayed on the site.
12. I am more likely to use an online Canadian pharmacy site if I am informed that this firm is an actual registered pharmacy as opposed to a pharmacy intermediary (affiliated middleman pharmacy).
13. I am more likely to use an online Canadian pharmacy if the site requires me to fill out a health profile before I can place an order.
14. I am more likely to use an online Canadian pharmacy if the site requires an original or copy of the prescription.

Personal Demographic. (on a scale from 1 to 5)

15. I am more likely to use an online Canadian pharmacy if the privacy policy states that it collects my email address.
16. I am more likely to use an online Canadian pharmacy if the privacy policy states that it collects my mailing address.
17. I am more likely to use an online Canadian pharmacy if the privacy policy states that it collects my telephone number.

18. I am more likely to use an online Canadian pharmacy if the privacy policy states that it collects my credit card number.
19. I am more likely to use an online Canadian pharmacy if the privacy policy states that it collects demographic information about me (age, gender, etc).

Computer Hardware/Software and Cookies Information. (on a scale from 1 to 5)

20. I am more likely to use an online Canadian pharmacy if the privacy policy states that it uses cookies.
21. I am more likely to use an online Canadian pharmacy if the privacy policy states that it uses cookies to track your computer's IP address.
22. I am more likely to use an online Canadian pharmacy if the privacy policy states that it uses cookies to collect usage tracking data.
23. I am more likely to use an online Canadian pharmacy if the privacy policy states that it uses cookies to collect domain name information.

Opt-In and Alter Ability. (on a scale from 1 to 5)

24. I am more likely to use an online Canadian pharmacy if the privacy policy states that the consumer can delete stored personal information from the site's database.
25. I am more likely to use an online Canadian pharmacy if the privacy policy states that the consumer can ALTER personal information from the site's database.
26. I am more likely to use an online Canadian pharmacy if the privacy policy states that it allows you to opt-out of their information collection process.
27. I am more likely to use an online Canadian pharmacy if the privacy policy states that it will not collect any information about you unless you give opt-in permission for this collection.

Disclosure of Information to Third Parties and Affiliates. (on a scale from 1 to 5)

28. I am more likely to use an online Canadian pharmacy if the privacy policy states that it does not disclose data to third parties.
29. I am more likely to use an online Canadian pharmacy if the privacy policy states that it discloses data to third parties.
30. I am more likely to use an online Canadian pharmacy if the privacy policy states that it only discloses information to outside parties if you consent to the release.
31. I am more likely to use an online Canadian pharmacy if the privacy policy states that it releases information to third parties in order to perform services for them.

32. I am more likely to use an online Canadian pharmacy if the privacy policy states that it releases information to third parties if legally required to do so.
33. I am more likely to use an online Canadian pharmacy if the privacy policy states that it releases information to third parties if the firm was acquired or merged.
34. I am more likely to use an online Canadian pharmacy if the privacy policy states that it releases information to associated affiliate firms.
35. I am more likely to use an online Canadian pharmacy if the privacy policy states that it absolves outside URL links from liability.
36. I am more likely to use an online Canadian pharmacy if the privacy policy states that it is not responsible for data that is collected by third-parties.

Security. (on a scale from 1 to 5)

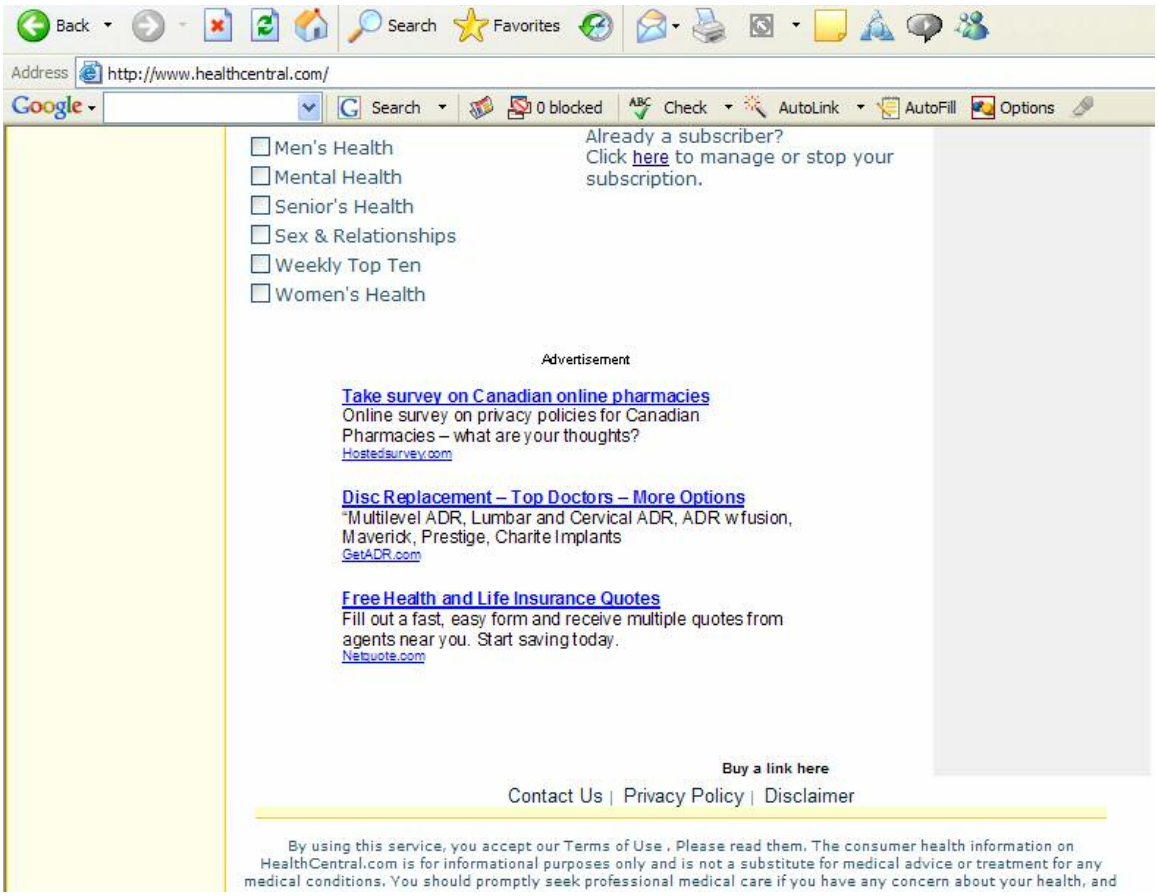
37. I am more likely to use an online Canadian pharmacy if the privacy policy states that it provides SSL/encryption security
38. I am more likely to use an online Canadian pharmacy if the privacy policy states that it only allows specific employees to access personal customer information.
39. I am more likely to use an online Canadian pharmacy if the privacy policy states that it has a password/login system for its customers.
40. I am more likely to use an online Canadian pharmacy if the privacy policy states that it protects the data with a firewall.
41. I am more likely to use an online Canadian pharmacy if the privacy policy states that it keeps its database/servers in a protected physical environment.

Miscellaneous Information. (on a scale from 1 to 5)

42. I am more likely to use an online Canadian pharmacy if the privacy policy states that it adheres to the COPPA law (does not collect information about children under 13 without the parents' permission).
43. I am more likely to use an online Canadian pharmacy if the privacy policy states that will post any changes to its privacy policy.
44. I am more likely to use an online Canadian pharmacy if there is an email or phone contact on the privacy policy page.

Appendix D

Screen Print of Online Advertisement in Healthcentral.com Web Site



Appendix E

IRB Approval

Name:	Joanne M. Kuzma
Maximum grade:	1
Date submitted:	December 15, 2004 2:29pm (Late)
Student files:	To view a file, click its filename.

Files	Modification date	Size
IRB for Research-Kuzma-12152004.doc	December 15, 2004 2:28pm	29.0 KB

Graded files:	None
Comments:	After reviewing your IRB Submission Form and Research Protocol I have approved your proposed research for IRB purposes. Your research has been determined to be exempt from further IRB review based on the following conclusion: Research using survey procedures or interview procedures where subjects' identities are thoroughly protected and their answers do not subject them to criminal and civil liability. Please note that while your research has been approved, additional IRB reviews of your research will be required if any of the following circumstances occur: 1. If you, during the course of conducting your research, revise the research protocol (e.g., making changes to the informed consent form, survey instruments used, or number and nature of subjects). 2. If the portion of your research involving human subjects exceeds 12 months in duration. Please feel free to contact me in the future if you have any questions regarding my evaluation of your research or the IRB process. Dr. Cannady ---------- James Cannady, Ph.D. Associate Professor Graduate School of Computer and Information Sciences Nova Southeastern University 954.262.2085 706.248.4250 (mobile phone) cannady@nova.edu PGP public key fingerprint: 8169 6D03 680E EF6C 899C 8C42 B4A3 DC9F 9F6B 4075 ----------
Grade:	**1** out of 1

Reference List

Adkinson, W., Eisenach, J., & Lenard, T. (2002, March). *Privacy online: A report on the information practices and policies of commercial Web sites*. The Progress & Freedom Foundation. Retrieved January 11, 2004 from http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf

Alexa Internet. (2005, March). *Dr. Koop's community Web rankings*. Retrieved March 28.2005 from http://www.alexa.com/data/details/main?q=drkoop&url=http://www.drkoop.com/

Alexander, P. (2001). The interface between consumers and commercial Internet sites: Information privacy concerns and fair information practice/privacy statements (Doctoral dissertation, University of Memphis, 2001). *Dissertation Abstracts International, 62*(02), 372A (UMI No. AAT 3003734)

Arrison, S. (2002, February). How you can protect your privacy. *Consumers' Research,* 10-13, 24.

Bahadur, G., Chan, W., & Weber, C. (2002, April 12). Privacy organizations and initiatives. *InformIT*. Retrieved January 19, 2004 from http://www.informit.com/isapi/product_id~%7B375B0072-9740-4090-9283-4EAB89BCEB35%7D/content/index.asp

Baumer, D., Earp, J., & Payton, F. (2000, December). Privacy of medical records: IT implications of HIPAA. *ACM SIGCAS Computers and Society 30*(4), 40-47.

BBBOnLine, Inc. (2004). *BBBOnLine Programs*. Retrieved January 18, 2004 from http://www.bbbonline.org/business/

Beales, H. (2002, March). *Privacy notices and the Federal Trade Commission's 2002 privacy agenda.* The Progress & Freedom Foundation. Retrieved October 1, 2004 from http://www.pff.org/publications/ecommerce/pop9.10privacyagenda.pdf

Bessell, T., Anderson, J., Silagy, C., Sansom, L., & Hiller, J. (2003, April). Surfing, self-medicating and safety: Buying non-prescription and complementary medicines via the Internet. *Quality and Safety in Health Care 12*(2), 88-93. Retrieved January 11, 2004 from Expanded Academic ASAP database.

Brown, W. (2002). Striking a balance: An application of gatekeeping theory to the issue of Internet privacy (Doctoral dissertation, University of North Carolina at Chapel

Hill, 2002). *Dissertation Abstracts International, 63*(08), 2735A (UMI No. AAT 3061664)

Cadogan, R. (2002). The ethics of data privacy in an electronic marketplace: A multiple case study of the privacy policy notice and the incorporation of fair information practice principles (Doctoral dissertation, Capella University). *Dissertation Abstracts International*, *62*(12), 4241A (UMI No. AAT 3037362)

California. Online Privacy Protection Act of 2003. (2003). *Ca. bus. & prof. code* s.s. 22575. Retrieved September 26, 2004 from http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=20719728778+0+0+0&WAISaction=retrieve

Canada. Parliament, Senate. Pharmaceutical sales to people in United States—Possibility of shortages, *Debates of the Senate* (Hansard), S. 2nd Session, 37th Parliament (2003). Retrieved September 29, 2004 from http://www.parl.gc.ca/37/2/parlbus/chambus/senate/DEB-E/094db_2003-11-04-e.htm

Canada Privacy Commissioner. (2002, January). *Privacy legislation in Canada*. Retrieved January 8, 2004 from http://www.privcom.gc.ca/fs-fi/02_05_d_15_e.asp

Canada Privacy Commissioner. (2003a). *A guide for individuals.* Retrieved April 10, 2006 from http://www.privcom.gc.ca/information/02_05_d_08_e.asp

Canada Privacy Commissioner. (2003b). *Privacy: Annual report to Parliament, 2002-2003*. Retrieved December 26, 2003 from http://www.privcom.gc.ca/information/ar/02_04_11_e.pdf

Canadian online pharmacy directory. (2004). CanadianOnlinePharmacyDirectory.com Home Page. Retrieved May 15, 2004 from http://www.canadianonlinepharmacydirectory.com

Canadian Pharmacists Association. (2004, January). *Complying with the pharmacist's privacy xode and PIPEDA: Guidelines and tools for pharmacists.* Retrieved January 10, 2004 from http://www.pharmacists.ca/content/hcp/resource_centre/practice_resources/pdf/PrivacyGuidelines_v1.pdf

Careerbuilder.com. (2004). *Search resume site*. Retrieved December 20, 2004 from http://www.careerbuilder.com/JobPoster/

Choy, A., Hudson, Z., Pritts, A., & Goldman, J. (2001, November). *Exposed online: Why the new federal health privacy regulation doesn't offer much protection to Internet users.* Institute for Health Care Research and Policy, Georgetown

University. Retrieved January 10, 2004 from http://www.healthprivacy.org/usr_doc/PIP_HPP_HealthPriv_report.pdf

Cohen, J. C. (2004, March/April). Pushing the borders: The moral dilemma of international Internet pharmacies. *Hastings Center Report,* 15-17.

Cox, B. (2002, July 15). Vitamin seller buys DrKoop domain. *Internetnews.com*. Retrieved March 28, 2005 from http://www.internetnews.com/ec-news/article.php/1404721

Culnan, M., & Bies, R. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59,* 323-342.

December, J. (2005). *Net use*. Retrieved August 10, 2005 from http://www.december.com/web/text/ tutor/netuse.html

Dienekis Information Systems. (2004). *Seventy percent of US consumers worry about online privacy*. Retrieved October 1, 2004 from http://www.dienekis.com/crm-news/EpkFEZykuAVy.php

Dixon, P. (2003, November 11). 2003 job search privacy study: Job searching in the networked environment: Consumer privacy benchmarks. *The World Privacy Forum*. Retrieved December 24, 2003 from http://www.worldprivacyforum.org/wpfjobstudy.pdf

Earp, J., & Baumer, D. (2003, April). Innovative Web use to learn about consumer behavior and online privacy. *Communications of the ACM*, *46*(4), 81-83.

Flammia, G. (2000, May/June). Privacy versus convenience. *IEEE Intelligent Systems, 15*(3), 12-13.

Fogg, B., Soohoo, C., Danielson, D., Marable, L., Stanford, J., & Tauber, E. (2002, October 29). How do people evaluate a Web site's credibility? *Consumer Webwatch News*. Retrieved November 14, 2004 from http://www.consumerwebwatch.org/news/report3_credibilityresearch/stanfordPTL.pdf

Fox, S. (2004a). *Prescription drugs online*. Pew Internet & American Life Project. Retrieved December 22, 2004, from http://www.pewinternet.org/pdfs/PIP_Prescription_Drugs_Online.pdf

Fox, S. (2004b, March 25). *Older Americans and the Internet*. Pew Internet & American Life Project. Retrieved August 17, 2005, from http://www.pewinternet.org/pdfs/PIP_Seniors_Online_2004.pdf

Fox, S., & Fallows, D. (2003). *Internet health resources*. Pew Internet & American Life Project. Retrieved December 24, 2004, from http://www.pewinternet.org/pdfs/PIP_Health_Report_July_2003.pdf

Fox, S., & Rainie, L., (2000). *The online health revolution: How the Web helps Americans take better care of themselves*. Pew Internet & American Life Project. Retrieved December 22, 2004, from http://www.pewinternet.org/pdfs/PIP_Health_Report.pdf

Goldman, J., Hudson, Z., & Smith, R. (2000, January). *Report on the privacy policies and practices of health Web sites*. California HealthCare Foundation. Retrieved January 10, 2004 from http://www.chcf.org/documents/ihealth/privacywebreport.pdf

Google.com. (2004). *Google home page*. Retrieved May 15, 2004 from http://www.google.com

Gordon, D. (2004, April). Surfing for drugs. *State Legislatures,* 28-29.

Graham, J. (2003, September). *Prescription drug prices in Canada and the United States – Part 4: Canadian prescriptions for American patients are not the solution*. Fraser Institute. Retrieved September 20, 2004 from http://www.fraserinstitute.ca/admin/books/files/PDP4John.pdf

Gregoire, L. (2003, April 1). Alberta MDs warned not to co-sign American prescriptions. *Canadian Medical Association Journal, 168*(7), 886.

Griggs, H. (2004, August 27). *Number of Americans without insurance reaches highest level on record*. Center on Budget and Policy Priorities. Retrieved August 17, 2005 from http://www.cbpp.org/8-26-04health.htm

HealthCentral.com. (2001, December). *MDchoice, Inc: A leading health information network, acquires HealthCentral.com* Retrieved March 28, 2005 from http://www.healthcentral.com/aboutus/PressRelease.html

Hochheiser, H. (2002, November). The platform for privacy preference as a social protocol: An examination within the U.S. policy context. *ACM Transactions on Internet Technology (TOIT), 2*(4), 276-306.

Hosmer, L. T. (1995). Trust: The connecting link between organizational theory and philosophical ethics. *Academy of Management Journal, 20,* 379-403.

Hsu, C. (2001). A cross-country examination of online privacy issues: From an adversarial paradigm toward a situational paradigm. A comparison of regulations, net users' concerns and practices, and Web sites' privacy statements in China, the Netherlands, Taiwan, and the United States (Doctoral dissertation, State

University of New York at Buffalo) *Dissertation Abstracts International, 64*(04), 1123A (UMI No. AAT 3089140)

Hu, J. (2003, December 24). Disney tweaks policy, shares user data. *News.com,* Retrieved January 18, 2004 from http://news.com.com/2100-1038-5133045.html?part=msnbc-cnet

Hubbard, W. K. (2003, March 27). Internet pharmacy consumer safeguards. *FDCH Congressional Testimony*. Retrieved December 10, 2004, from EBSCOhost databases.

IMS Health Canada. (2005, March 7). *Retail prescriptions grow 5.6% in 2004, down 7.9% in 2003*. Retrieved November 5, 2005 from http://www.imshealthcanada.com/htmen/1_0_16.htm

Kobsa, A. (2002, May). Personalized hypermedia and international privacy. *Communications of the ACM*, *45*(5), 64-67.

Korcok, M. (2002, October 29). Forget U.S. politicians' promises – Canada still cheap-drug Mecca. *Canadian Medical Association Journal, 167*(9), 1044.

Korcok, M. (2003, November 11). U.S. states ponder buying drugs from Canada. *Canadian Medical Association Journal, 169*(10), 1065.

Korcok, M. (2004). Internet pharmacy: The tug-of-war intensifies. *Canadian Medical Association Journal, 170,* 946-947.

Krauss, C. (2004, December 11). Internet drug exporters feel pressure in Canada. *New York Times,* pp. A1, A5.

Kristol, D. (2001, November). HTTP cookies: Standards, privacy and politics. *ACM Transactions on Internet Technology (TOIT), 1*(2), 151-198.

Larson, L., Larson, R., & Greenlee, J. (2003, June). Privacy protection on the Internet. *Strategic Finance, 84*(12). Retrieved January 18, 2004 from ProQuest database.

Lee, Y. (2002). Internet privacy and electronic commerce: Meeting the challenge of self-regulation in a digital environment (Doctoral dissertation, Indiana University). *Dissertation Abstracts International*, *63*(05), 1611A (UMI No. AAT 3054408)

Leizerov, S. (2001). The institutionalization of conflicts in cyberspace: A study of the conflict over online privacy (Doctoral dissertation, George Washington University). *Dissertation Abstracts International*, *62*(2), 679A (UMI No. AAT 3003055)

Manitoba still tops for Internet drug sales to US, but Alberta and BC have highest growth rate. (2004, April 1). *Canada NewsWire*. Retrieved September 29, 2004 from http://www.newswire.ca/en/releases/archive/April2004/01/c6831.html

McCullagh, D. (2004, January 8). Treasury breaks word on e-mail anonymity. *MSNBC.COM*. Retrieved January 9, 2004 from http://www.msnbc.msn.com/id/3909094/

McCutcheon, J. (2002, November 4). *Compliance and the new privacy sector laws.* Blaney McMurty LLP. Retrieved January 12, 2004 from http://www.blaney.com/files/article_privacy_compliance.pdf

MDchoice.com. (2001, May). *MDchoice.com's acquisition of HealthScout Network makes it top-five consumer health channel*. Retrieved March 28, 2005 from http://www.mdchoice.com/pt/consabout/Press9.asp

Meadows, M. (2002, September-October). Imported drugs raise safety concerns. *FDA Consumer Magazine.* Retrieved January 8, 2004 from http://www.fda.gov/fdac/features/2002/502_import.html

Mears, R., MacNeil, E., & DeJamette, K. (2003, March). A matter of trust. *Optimize.* Retrieved December 20, 2004 from http://www.optimizemag.com/showArticle.jhtml?articleID=17700867

Moores, T., & Dhillon, G. (2003, December). Do privacy seals in e-commerce really work? *Communications of the ACM*, *46*(12), 265-271.

National Association of Boards and Pharmacy. (2004). *VIPPS information and verification Site.* Retrieved January 6, 2004 from http://www.nabp.net/vipps/intro.asp

National Research Federation. (2004, May). *Online retail sales and profitability on the rise*. Retrieved November 5, 2005 from http://retailindustry.about.com/od/seg_internet/a/bl_nrf052504.htm

New mood in Washington to approve drug importation magnifies risk to Canada's drug care system. (2004, May 17). *Canada NewsWire.* Retrieved September 29, 2004 from http://www.newswire.ca/en/releases/archive/May2004/17/c3977.html

Olsen, S. (2000, July 12). Nearly undetectable tracking device raises concern. *CNET News.com*. Retrieved January 19, 2004 from http://news.com.com/2100-1017-243077.html?legacy=cnet

Parloff, R. (2004, March 8). The new drug war. *Fortune, 149*(5) 144-150.

Pennington, R., Wilcox, H. D., & Grover, V. (2003/2004). The role of system trust in business-to-consumer transactions. *Journal of Management Information Systems, 20,* 197-226.

PharmacyChecker.com. (2003a, November 6). *New survey of Canadian online pharmacies finds only 30% are licensed and provide important consumer protections.* Retrieved December 23, 2003 from http://www.pharmacychecker.com/news/news_110603.asp

PharmacyChecker.com. (2003b, April 7). *Fifty percent of Internet pharmacies not licensed*. Retrieved December 23, 2003 from http://www.pharmacychecker.com/news/news_040703.asp

PharmacyChecker.com. (2003c, November). *Sample profiles*. Retrieved December 23, 2003 from http://www.pharmacychecker.com/sampleprofile.asp

PharmacyChecker.com. (2003d). *About online pharmacies: What you need to know.* Retrieved January 6, 2004 from http://www.pharmacychecker.com/aboutop.asp

PharmacyChecker.com (2003e). *PharmacyChecker.com predicts that billions can be saved and consumers using U.S. wholesale pharmacies for generics and Canadian pharmacies for branded medications.* Retrieved January 26, 2004 from http://www.pharmacychecker.com/news/news_072303.asp

Poll: Public supports healthcare for all. (2003, October 19). *USA Today.* Retrieved September 19, 2004 from http://www.usatoday.com/news/health/2003-10-19-health-poll_x.htm

Privacilla.org (2002, April). *What is Privacilla*? Retrieved December 30, 2005 from http://www.privacilla.org/about/whatis.html

Privacilla.org (2003, November). *Affiliate-sharing and consumers: How "privacy" regulation misses the mark, hits marketing*. Retrieved January 10, 2004 from http://www.privacilla.org/releases/Affiliate-Sharing_Report.html

Privacyalliance.org. (2003a). *Guidelines for online privacy policies*. Retrieved August 11, 2004 from http://www.privacyalliance.org/resources/ppguidelines.shtml

Regan, K. (2003, May 9). U.S. to probe Microsoft Passport flaw. *ECT News Network*. Retrieved September 19, 2004 from http://www.technewsworld.com/story/21481.html

Reisch, L. A. (2003). Potentials, pitfalls, and policy implications of electronic consumption. *Information & Communication Technology Law, 12,* 93-109.

Resnick, M. L., & Montania, R. (2003). Perceptions of customer service. Information privacy, and product quality from semiotic design features in an online Web store. *International Journal of Human-Computer Interaction, 16,* 211-234.

Rose, E. (2000, June). Balancing Internet marketing needs with consumer concerns: A property rights framework. *ACM SIGCAS Computers and Society*, *30*(2), 20-24.

Rothstein, N. (2001, March). Protecting privacy and enabling pharmaceutical sales on the Internet: A comparative analysis of the United States and Canada. *Communications Law Journal*, *53*(2), 188-221. Retrieved January 10, 2004 from Expanded Academic ASAP database.

Stein, T. (2003, March). Lack of trust threatens online-commerce success. *Optimize.* Retrieved December 20, 2004, from http://www.optimizemag.com/showArticle.jhtml?articleID=17700878

Sweet, M. (2001). *Policing online pharmacies: Bioterrorism meets the war on drugs.* Duke University, School of Law. Retrieved January 7, 2004 from http://www.law.duke.edu/journals/dltr/articles/PDF/2001DLTR0041.pdf

Thibodeau, P. (2001, May 7). FTC official faults corporate privacy policies. *Computerworld.* Retrieved August 12, 2004 from http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,60248,00.html

Thompson, C. (2004, February 15). Drug importation raises issues for pharmacists. *American Journal of Health-System Pharmacy, 61*(4), 328-330.

TRUSTe. (2004). *Privacy seal programs.* Retrieved January 18, 2004 from http://www.truste.com/consumers/seal_programs_overview.php

U.S. Bureau of the Census. (2005, August 30). *Income stable, poverty rate increases, percentage of Americans without health insurance unchanged*. Retrieved October 13, 2005 from http://www.census.gov/Press-Release/www/releases/archives/income_wealth/005647.html

U.S. Congress, House. (2003). *International prescription drug parity: Are Americans being protected or gouged? Hearings before the Committee on Government Reform*, *House of Representatives,* 108th Cong., 1st sess.

U.S. Congress, Senate. *Comparative pricing of prescription drugs sold in the United States and Canada and the effects on U.S. customers: Hearings before the Subcommittee on Consumer Affairs Foreign Commerce and Tourism of the Committee on Commerce, Science, and Transportation,* 107th Cong., 1st sess. (2001). Retrieved September 19, 2004 from http://purl.access.gpo.gov/GPO/LPS29701

U.S. Federal Trade Commission. (1999, November). *How to comply with the Children's Online Privacy Protection Rule.* Washington: The Commission. Retrieved January 19, 2004 from http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm

U.S. Federal Trade Commission. (2000, May). *Privacy online: Fair information practices in the electronic marketplace: A report to Congress.* Washington: The Commission. Retrieved January 10, 2004 from http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

U.S. Federal Trade Commission. (2000b, July). *Online pharmacies settle FTC charges.* Washington: The Commission. Retrieved January 11, 2004 from http://www.ftc.gov/opa/2000/07/iog.htm

U.S. Federal Trade Commission. (2002c, April). *Microsoft settles FTC charges alleging false security and privacy promises.* Washington: The Commission. Retrieved October 1, 2004 from http://www.ftc.gov/opa/2002/08/microsoft.htm

U.S. Federal Trade Commission. (2002d, August 8). *Protecting children's privacy under COPPA: A survey on compliance.* Washington: The Commission. Retrieved October 1, 2004 from http://www.ftc.gov/os/2002/04/coppasurvey.pdf

U.S. Federal Trade Commission. (2004, June). *The FTC and consumer privacy: An accomplished agenda.* Washington: The Commission. Retrieved October 1, 2004 from http://www.ftc.gov/speeches/beales/0406conprivacyaccomplished.pdf

U.S. General Accounting Office. (2000, October 19). *Internet pharmacies—adding disclosure requirements would aid state and federal oversight.* Retrieved December 10, 2004, from www.gao.gov/cgi-bin/getrpt?GAO-01-69

U.S. White House, Office of the Press Secretary. (1999, December 28). The Clinton administration unveils new initiative to protect consumers buying prescription drug products over the Internet. U.S. Food and Drug Administration. Retrieved January 7, 2004 from http://www.fda.gov/oc/buyonline/onlinesalespr.html

Vivian, J. (2003, July 15). Canadian drug imports. *U.S. Pharmacist*, *28*(7). Retrieved June 2, 2004 from http://www.uspharmacist.com/index.asp?show=article&page=8_1113.htm

Volokh, E. (2000, August). Personalization and privacy. *Communications of the ACM*, *43*(8), 84-88.

W3C. (2002). *Summary report: W3C workshop on the future of P3P*. Retrieved March 28, 2005 from http://www.w3.org/2002/12/18-p3p-workshop-report.html

W3C. (2003, December 2). *Platform for privacy preferences (P3P) project*. Retrieved January 18, 2004 from http://www.w3.org/P3P/

Webster, P. (2003, November 29). FDA chief attacks Canada's drug price controls. *The Lancet 362*(9398),1816.

Whitwham, B. (2003a, March 18). Dispute over Canada's online pharmacies heating up. *Canadian Medical Association Journal, 168*(6), 759.

Whitwham, B. (2003b, April 15). US voters' love of Canada's Internet drugstores making politicians cautious. *Canadian Medical Association Journal, 168*(8), 1033.