Project Number: KJR-1101

Internet Privacy

Public Perceptions of Security and Convenience

An Interactive Qualifying Project Report

submitted to the Faculty

of

WORCESTER POLYTECHNIC INSTITUTE

in partial fulfillment of the requirements for the

Degree of Bachelor of Science

by

Dunia Abdulrazak, Klevis Luli, and Marc Michaud

Approved:

Professor Kent J. Rissmiller, Project Advisor

ABSTRACT

The purpose of this study is to determine how Internet users' educational background, gender, and amount of time spent online affect their preference for privacy or convenience within the services of social networking, e-commerce, and online banking. A survey and interviews were conducted to determine users' viewpoints and awareness of potential online threats. We found a relationship between time spent online and users' perceived privacy knowledge and concluded that most users exhibit a "mild" level of concern online.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

When the Internet was first introduced, it was a popular and important service that had not yet become integrated into peoples' lives. As the Internet became an essential part of users' lives, privacy issues began to emerge between Internet users and online service providers. Within the context of this paper, Internet privacy shall be defined as the implicit right of individuals to be able to control their degree of exposure in regards to their information when using the Internet.

While Internet privacy has received significant attention as a topic of research and is becoming popular in the media, it is also a topic of which many are oblivious. Advances in technology, such as automated data mining tools, allow online service providers and data aggregators to collect and process an individual's online information more quickly and efficiently than ever before. As these technologies and features were incorporated online, the environment of the Internet began to change, leading to the rise of privacy concerns. In spite of efforts to resolve these privacy issues by developing privacy policies, these policies are constantly changing their terms of service. Without proper knowledge of these continuous changes online, people are not able to fully understand how their privacy may be at risk, which is why it is important to make sure people are informed about these changes and possible risks.

The purpose of this paper is to determine the factors that influence a person's desire for convenience or privacy when using the popular online services of social networking, e-commerce, and online banking. This includes examination of users' knowledge about the risks associated with these services, as well as the level of privacy concern they exhibit.

The first section of this report offers background on the conveniences and risks associated with the use of social networking, e-commerce, and online banking. This section also

includes information about Internet literacy, and presents relevant literature for this study. The second section of this report explains the research methods used during this study, which consist of an online survey and series of interviews. The third section of this report describes the data collected from the survey and interviews, including the plan used for data analysis and the concluding results. The last section of this report details conclusions drawn from the data analyses, as well as concluding thoughts on the issue of Internet privacy. This final section also includes remarks about the accuracy of the testing instruments, as well as goals for further research.

2. BACKGROUND AND LITERATURE REVIEW

This section of the report will provide information on various online services, privacy issues concerning these services, privacy policies and the effect of Internet literacy, regarding these issues. The overall goal of this section is to provide a clear background for this research study.

2.1 CONVENIENCES AND RISKS

The Internet is a major tool that eases the lives of millions of people all over the world, and provides users with many conveniences, ranging from the ability to stream movies online or manage bank accounts. Convenience within the context of this paper is defined as an online tool that allows users to complete a task with little effort. In addition to the conveniences that the Internet provides, it also makes the user vulnerable to risks, which could bring harm to an individual.

A risk is defined as an action or activity, having the potential to trigger an undesirable outcome. One example of a risky action would be exposing personally identifiable information (PII) online, which could lead to serious consequences, such as identity theft, abuse of an individual, or loss of financial assets.

In this paper, the conveniences, risks, and consequences of three major online services are explored: social networking, electronic commerce (e-commerce), and online banking. Social networking is an online service that establishes connections among individuals, allowing them to share their interests or activities. E-commerce refers to services used for buying or selling goods over the Internet, and online banking is a service that allows individuals to manage their bank accounts and finances, regardless of physical location.

Social Networking

Social networking sites, such as Myspace, Facebook, and Twitter have introduced the concept of interacting and socializing with people online. In some ways, social networking has become a daily part of many people's lives, especially the lives of teenagers and young adults. It provides users with the convenience of being able to stay up-to-date on their friends' activities, determine the availability of all their friends, and meet thousands of people in one place in hopes of establishing or renewing relationships.

Before the occurrence of social networking, a person would have to talk to another individual in order to socialize and develop a social relationship. Additionally, before social networking, Internet users would either email or instant message (IM) each other as a means of communication, but the user would have to visit a different website in order to perform each task. Social networking provides individuals with the convenience of communicating with each other online through private messages, instant messages, and public posts, all from just one website.

The privacy issues relating to the use of social networking sites arises from the concepts of fake profiles and tagging. Tagging is a feature that allows friends to associate each other with activities, events, or photographs without prior notice. Additionally, in order to create a profile on any social networking site, only a valid email address is required, allowing anyone to pretend to be someone they are not online. The concepts creating fake profiles and tagging, combined with weak privacy policies, can put an individual at risk due to loss of privacy. One example of such an event could occur if someone was tagged in an image that was of an unprofessional nature and was later seen by a potential employer. The resulting consequence could be the loss of

a job opportunity. Although this may not appear to be a significant threat towards an individual's privacy, the potential of having their privacy invaded exists.

Electronic Commerce (e-commerce)

The idea of online shopping, or electronic commerce, has launched an entirely new business venue and made it easier for people to shop. In previous practices, people would have to drive from store to store in order to purchase the items they desired, but now they have the convenience of making their purchases from anywhere, through the Internet. Websites such as E-bay.com and Amazon.com are just two examples of widely used e-commerce sites today, which allow individuals to purchase items from other people or suppliers. E-commerce has also allowed major store-chains to have an online presence in order to expand their markets, allowing individuals to have another, more convenient method of obtaining their goods.

Despite the convenience of purchasing items online and receiving exclusive discounts, e-commerce introduces serious risks that could affect a person's privacy. When a person registers with an e-commerce site, personal information of a more sensitive nature is required, thus escalating the level of risk and possible consequences for the person. This information can include, but is not limited to, personally identifiable information (PII) and billing & shipping information, which includes credit and debit card account information.

The privacy issue within the service of e-commerce resides in the fact that a person's billing and shipping information is usually stored online, along with his or her purchase history. As a result, if there was an issue with the security of the payment services' systems, or if the user was not cautious, another person could compromise that individual's log-in information and gain access to his or her personal and billing information. According to the Anti-Phishing Working Group (APWG) *"2nd Half Phishing Activity Trends Report,"* the industry of payment services

was the second highest target for phishing attacks, between the months of August and December in the year 2010 (Manning, 2011). Phishing is a technique by which a person is misdirected into providing sensitive information, by crafted emails or websites that resemble that of the actual online service providers.

The consequences resulting from becoming a victim of a phishing attack can potentially ruin a person's financial assets, such as having their credit history damaged or having their accounts cleared. Additionally, the consequences could be as severe as identity theft, depending on the extent of information that was stored online. E-commerce poses a threat to people's privacy when using the Internet, because it makes them vulnerable to phishing attacks, thus putting a user's personal and billing information at risk of being compromised.

Online Banking

Online banking has revolutionized the way individuals can interact with their bank, as well as how they manage their bank accounts. Through the use of the Internet, online customers have the opportunity to pay their bills, review their statements, and transfer money online through their bank's website. These conveniences relieve users from having to perform tedious and time-consuming tasks, such as waiting in line for a teller, balancing a checkbook or periodically mailing bill payments.

Online banking has become a widely-known option, available to anyone with a bank account and a valid email address. However, by making this information accessible from the Internet, customers put their privacy in jeopardy and become more vulnerable to malicious attacks, such as phishing and the interception of sensitive information. According to the Anti-Phishing Working Group, between the months of June and December in the year 2010, financial services were determined to be the industry that was the greatest target for phishing (Manning,

2011). As a result, when an online user registers for the service of online banking and is deceived by a phishing email, he or she could suffer severe consequences, such as identity theft and the loss of financial assets. In other words, online banking makes users more vulnerable to phishing attacks, which puts their privacy, identity, and financial assets at risk.

2.2 PRIVACY POLICIES

While there is some legislation that enforces privacy within the services of social networking, e-commerce, and online banking, Internet privacy is primarily self-regulated by the industry. In an attempt to address privacy concerns within the use of these services, along with others, companies create a terms of service agreement. This agreement, between a company and its users, details the use of the provided service, relevant privacy and security policies, and the user's liabilities and rights. However, this method of resolving privacy concerns by creating terms of service agreements has proven to be problematic. This is due to the advances in technology and the growth of the Internet, which both greatly impact information flow online. Advertisers, mobile apps, social networks, e-commerce, and online banking are all new trends in the online industry, whose success is based on the usage of data taken from users with or without their consent.

In order to resolve the privacy concerns that arise with the use of an online service, the Federal Trade Commission (FTC) has enforced federal laws to restrict the disclosure of consumer information and require companies to ensure the security and integrity of the data collected. One example of these laws is Title V of the Gramm-Leach-Bliley Act, which states that customers' financial information must be restricted under privacy provisions when being disclosed to third parties (Federal Trade Commission, 2001). This law addresses the issue of how a person's financial information is securely distributed online, which means that companies are

regulated in how they collect and utilize users' private information. This addresses the risks that arise from the use of e-commerce and online banking services. Since the January 2011, Congress (112th Congress) has introduced several laws to address the risks that modern society is exposed to, as well as create a baseline for industries to follow in order to address privacy concerns (Table 1). However, most of these bills have not made any progress after being referred to House committees and are then discarded.

Bill (Sponsor)	Summary, Committee(s) of Referral, and Status as of October 7, 2011
H.R.654 (Speier, Jackie)	**Do Not Track Me Online Act**. Requires the Federal Trade Commission (FTC) to promulgate regulations to establish standards for the required use of an online opt-out mechanism to allow a consumer to prohibit the collection or use of any covered information and to require a covered entity to respect the choice of such consumer to opt-out of such collection or use. (Commerce, Manufacturing, and Trade.)
S.799 (Kerry, John F.)	**Commercial Privacy Bill of Rights Act of 2011**. Directs the Federal Trade Commission (FTC) to initiate a rulemaking requiring security measures to be carried out by any person (defined in this Act as a "covered entity") collecting, using, transferring, or storing certain personal information concerning over 5,000 individuals… (Commerce, Science, and Transportation)
S.1223 (Franken, Al)	**Location Privacy Protection Act of 2011**. Amends the federal criminal code to prohibit a nongovernmental individual or entity engaged in the business of offering or providing a service to electronic communications devices from knowingly collecting, obtaining, or disclosing to a nongovernmental individual or entity geolocation information from an electronic communications device without the express authorization of the individual using the device. (Judiciary)
H.R.1841 (Stearns, Cliff)	**Data Accountability and Trust Act (DATA) of 2011**. Requires the Federal Trade Commission (FTC) to promulgate regulations requiring each person engaged in interstate commerce that owns or possesses electronic data containing personal information to establish security policies and procedures. (Commerce, Manufacturing, and Trade)

Table 1: Bills introduced in the 112th Congress

2.3 INTERNET LITERACY

Internet literacy is defined as the ability to use the Internet proficiently and securely as a result of how familiar and knowledgeable a person is, in regards toward the Internet. In other words, for an individual to be considered Internet-literate, the individual must be familiar with the practices used to protect privacy online, as well as the risks that follow the use of online services.

As the complexity of the Internet increases over time, people are often left uneducated as to the new risks and consequences that develop with the growth of the Internet. As a result, people may see only the benefits offered by social networking, e-commerce, and online banking services, without realizing the full extent of the consequences that follow.

2.4 RELEVENT LITERATURE

An example of a previous study done in order to examine whether the conveniences provided within online services are worth the risks, is seen in the Social Science Computer Review conducted by O'Neil titled, *"Analysis of Internet Users' Level of Online Privacy Concerns*" (O'Neil, 2001). In this study, levels of concern relating to online privacy across four demographic groups were explored: gender, education level, income level, and race. Additionally, the study explores what the most critical issue facing the Internet is, the level of concern respondents have toward online security of their personal information, and whether convenience or privacy is more important to the respondents.

The results gathered from the O'Neil study indicate that race may have an impact on a person's level of concern about Internet privacy. However, the conclusion that Whites are more concerned about privacy online, compared to other races, was a result of possible biasing, since only 13.4% of the respondents were a race other than White. Additionally, it was determined that

females exhibited a higher concern for privacy online compared to males. The O'Neil study also concluded that respondents with a higher level of education were more concerned about Internet security, and that income does not have an effect on a person's concern about privacy online. O'Neil also came to the conclusion that privacy online was the most critical issue facing the Internet, according to the responses received, and that approximately three-quarters of the study's participants valued privacy more than convenience.

Another major focus of previous research studies has been centered on determining which factors, and how strongly these factors, influence a person's knowledge about Internet privacy. One example of such a study is seen in The International Journal of Human-Computer Studies conducted by Jensen titled *"Self-Reports Versus Observed Behavior"* (Jensen, 2005). In this study, participants were asked a series of questions related to Internet privacy in order to establish their knowledge level, and to gauge the knowledge level of an average Internet user. This study also examined the effect of gender on Internet privacy knowledge levels, as well as the differences in concern on various privacy issues. However, Jensen's study proved to have biasing in its results, considering that the sample population was evaluated to be more knowledgeable on the topic of Internet privacy compared to the "average" user. This bias was then minimized by categorizing the participants into groups based on knowledge levels.

The results gathered from the Jensen study indicates that there is no distinct difference in knowledge levels among different privacy groups. In other words, those respondents who were more concerned about Internet privacy were not smarter than those who were not concerned about privacy, and vice-versa. Additionally, Jensen's study suggests that females have a higher level of concern about Internet privacy compared to males, as seen in the O'Neil study.

A similar study, which examined the differences in privacy concerns among different countries rather than genders, is seen in Zhang's study from the Journal of Internet Commerce, titled *"Characteristics of Internet Users and their Privacy Concerns"* (Zhang, 2008). In this study, college students from America and China were questioned in regards to their concerns within the topic of Internet privacy. The study concluded that Chinese students were more likely to share personal information online compared to American students. Zhang's study also confirmed the results from the O'Neil study, stating that income does not have an effect on a person's knowledge level or concern about Internet privacy.

Additionally, an IEEE study by Earp titled, *"Examining Internet Privacy Policies Within the Context of User Privacy Values,"* examined the three most influential factors that lead a person to trust a website (Earp, 2005). The data gathered within the study determined that a company's name, the ability to opt-out of data collection, and the presence of a privacy policy on the site is what influences a person's decision in trusting their information online within a particular website.

Concluding Remarks

Upon studying literature based on the topic of Internet privacy, researchers have found that a relation exists between a person's concern and knowledge level regarding the Internet. Researchers have also determined that certain factors, such as gender and education, affect peoples' levels of concern online. However, these past studies, specifically the O'Neil and Jensen study, only gauge peoples' privacy concerns in general and do not consider that their privacy concerns may differ among various online services. This limits the scope of both the O'Neil and Jensen study, since the researchers do not take into account that a person's privacy concerns can change depending on certain situations. In other words, a person's concern for

privacy may change depending on the situation or type of data that he or she provided online. Our study will determine how concerned Internet users are about social networking, e-commerce, and online banking. Furthermore, our study intends to determine what factors affect a person's level of concern and knowledge regarding the Internet.

3. METHODOLOGY

The main topic of research for this paper was to determine whether people valued convenience or privacy more when using various Internet services. In order to gather data for this research, two methods were used, a survey and interviews. These methods were chosen among others, in order to allow various people to be contacted as participants. Through the use of these research methods, participants were assessed on how knowledgeable they were about the topic of Internet privacy. Additionally, the participants were observed to determine if informing a user about the risks that follow the use of various Internet services, would change their opinion or usage of these services. These methods would also determine how concerned a participant is about his or her privacy online.

3.1 ONLINE SURVEY

Purpose

The purpose of the online survey was to collect demographic information on participants, determine how knowledgeable they are about Internet privacy, and observe if any potential changes in their online behaviors may occur as a result from taking the survey. In other words, the online survey would determine whether educational background, gender, level of privacy concern, or the amount of time spent online influences a person's desire for convenience or privacy, their knowledge level, and their online behaviors.

Method

The survey was developed using Google Docs and was divided into three different sections. The first section asked the participant a series of multiple choice questions regarding their age, education level, and general demographic information. This portion of the survey also gathered data on the participant's use of the Internet regarding the amount of time spent online

each day. The purpose of this section of the survey was to determine if demographic information had an effect on participants' knowledge level about Internet privacy, and their preference regarding convenience or privacy. The entire set of questions included in the survey is provided in Appendix A.

The second portion of the survey asked the participant a series of questions regarding the Internet. The data collected from this section of the survey was used to categorize participants based on their level of privacy concern. The questions used to categorize the participants were based on Jensen's study titled *"Self-Reports Versus Observed Behavior"* (Jensen, 2005). In Jensen's study, respondents were asked to assess their concerns on various privacy issues, by choosing one of the following responses: Agree, Neutral, and Disagree. Then, depending on the participant's response, they were categorized into groups based on their privacy concerns. These categories were defined as: Privacy Fundamentalist, Privacy Pragmatist, and Privacy Unconcerned. In order to categorize the participants of our study, participants were asked to rate their level of concern on various aspects of the Internet on a scale of "Strongly Agree" to "Strongly Disagree," as seen in the following question:

Here are some statements about the internet. Do you agree strongly, agree somewhat, disagree somewhat, or disagree strongly.
Please answer for each statement.

	Strongly disagree	Somewhat disagree	Somewhat agree	Strongly agree
The providers of on-line services should be able to track the places users go on the Internet in order to send these users targeted marketing offers.	○	○	○	○

If the participant answered “Strongly Disagree” to the question listed above, they would be declared “Privacy Fundamentalist,” since they demonstrate a high level of concern about the Internet. However, if the participant answered “Strongly Agree,” they were considered “Privacy Unconcerned,” due to their low level of privacy concern, and those that answered with a combination of privacy and non-privacy oriented answers were considered “Privacy Pragmatists.” The purpose of this section of the survey was to determine how concerned participants are about privacy online, as well as verify whether privacy concern affected a person’s online behavior.

The last portion of the survey assessed how knowledgeable participants were about Internet privacy within the services of social networking, online banking, and e-commerce. The data collected from this section determined the steps participants take towards protecting themselves from potential harms online, and aided us in determining which online service raises the most privacy concern. This section also examined if users of these Internet services may change their opinion or use of services after being informed of the risks that follow. The purpose of this section of the survey was to determine how concerned participants are about privacy within the services of social networking, online banking, and e-commerce. Additionally, this portion of the survey examined whether convenience or privacy is more important to participants, as well as their desire to change the use of popular online services after being informed about the corresponding risks.

Outcomes

With the online survey, multiple outcomes were expected. One of these outcomes was that Worcester Polytechnic Institute students would claim to be more knowledgeable about Internet privacy and protecting themselves from online threats compared to non-WPI

participants. This is a preferred outcome because Worcester Polytechnic Institute students are believed to have a higher familiarity with technology due to their education compared to non-WPI participants.

The next expected outcome was that those participants who were categorized as Privacy Fundamentalists would be more knowledgeable about the risks following the use of Internet services compared to the Privacy Unconcerned participants. This is a preferred outcome because those participants who are knowledgeable and aware about the risks associated with the Internet, are likely to be concerned about privacy online.

Another preferred outcome was that a majority of the survey population would reconsider the use of social networking, e-commerce, or online banking after becoming informed about the current risks following these services. This would then imply that the survey participants are concerned about their privacy online.

It is also expected that the more time a person spends online, the more knowledgeable he or she becomes about Internet privacy and protecting themselves from online threats. This would imply that the amount of time a person spends on the Internet affects their knowledge about privacy issues, which then allows the person to adequately protect themselves online.

Distribution

In order to distribute the survey, two online sources were utilized. The first method of distribution was the undergraduate alias at Worcester Polytechnic Institute, which represented the main group of participants during this study. Worcester Polytechnic Institute was chosen because of its strong emphasis on technology and the ability to easily communicate with students. The other method used to distribute the survey was social networking sites, in order to allow for more responses. The survey remained online for a total of thirty-eight days, and

received a total of three-hundred and eighty-eight responses.

Additionally, by distributing the survey through social networking sites, another group of participants were able to be represented in the study, which were people not attending Worcester Polytechnic Institute. This minimized the amount of biasing that could have occurred if the participants consisted of only people with a strong background in technology, such as the students attending Worcester Polytechnic Institute.

3.2 INTERVIEW

Purpose

The purpose of conducting interviews was to reinforce the results gathered from the online survey, and to receive more in-depth responses from the participants.

Method

The interview questions were designed to be very similar to those of the online survey, with only two major differences. The first difference was that the interview did not contain any questions about the participant's demographics. The second difference was that the questions chosen for the interview were rewritten as open-ended questions, in order to allow for richer responses relating to the participant's view on Internet privacy and their online behaviors. The entire set of questions included in the interview can be found in Appendix B.

Interview Subjects and Location

The participants for these interviews consisted of students from the Psychology Pool at Worcester Polytechnic Institute. The Psychology Pool consists of undergraduate students who were currently enrolled in a psychology class at the time.

The interviews took approximately fifteen minutes and took place in various tech suites, which are rooms that can be reserved for education purposes, at Gordon Library, which is

located on the Worcester Polytechnic Institute campus.

Additionally, in order to eliminate any biasing of the participants' responses, the interviews were conducted individually, with a total of four participants.

Interviewing Procedure

The interview began by informing the participant that all their responses would remain confidential, and that they would be recorded. The interviews were conducted by reading off a pre-written script containing the order of questions to be asked. Additionally, the participants were recorded on two laptops using the Audacity software program.

The first set of questions asked during the interview regarded the amount of time the participant spent online each day and their familiarity on the topic of Internet privacy. This set of responses would establish how Internet-literate the participant was, and determine if there exists a relation between a participant's knowledge about the Internet and the amount of time they spend online. The next set of questions asked the participant for their opinions on various aspects of the Internet. This set of responses would then allow the participant to be categorized as Privacy Fundamentalist, Privacy Pragmatist, or Privacy Unconcerned, and verify if a person's privacy views relates to their online behaviors.

After that, participants were questioned about their ability to protect themselves online through the use of protective software, as well as whether they valued convenience or privacy. This set of responses would then verify if there is a correlation between privacy views and a person's tendency to value convenience or privacy more. Additionally, the responses received would determine if a correlation exists between a person's familiarity with the Internet and their ability to protect themselves online. The interview then concluded with a series of questions regarding the use of social networking, e-commerce, and online banking. This last portion of the

interview would determine what characteristics make a person more vulnerable to having their personal information becoming compromised online.

4. RESULTS AND DISCUSSION

4.1 ONLINE SURVEY ANALYSIS

Privacy View Analysis

In order to investigate the effect a person's privacy view has on their online habits, the survey population was divided into three classes (Fundamentalist, Pragmatist, and Unconcerned) based on their responses to the following question:

Here are some statements about the internet. Do you agree strongly, agree somewhat, disagree somewhat, or disagree strongly.
Please answer for each statement.

	Strongly disagree	Somewhat disagree	Somewhat agree	Strongly agree
The providers of on-line services should be able to track the places users go on the Internet in order to send these users targeted marketing offers.	○	○	○	○
Consumers have lost all control over how personal information is collected and used by companies.	○	○	○	○
Most businesses handle the personal information they collect about consumers in a proper and confidential way.	○	○	○	○
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	○	○	○	○

Participants were determined to be Privacy Fundamentalists if they responded to these questions with the following answers: Somewhat/Strongly Disagree, Somewhat/Strongly Agree, Somewhat/Strongly Disagree, and Somewhat/Strongly Disagree. Those participants who

responded with the inverse of the Fundamentalists' responses were then considered Privacy Unconcerned, whereas the participants who answered with a mixture of Fundamentalist and Unconcerned responses or responded with answers that did not represent a specific privacy view were then determined to be Privacy Pragmatists.

Once the survey participants were categorized, it was determined (Figure 1) that the most represented privacy group was Pragmatists (69.6%), whereas the least represented was Unconcerned (2.6%).

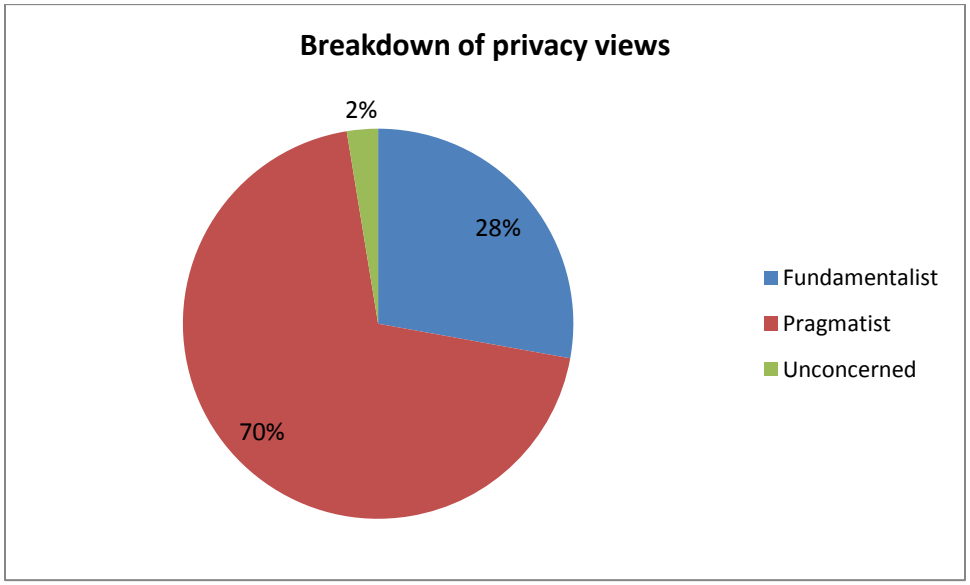

Figure 1: Breakdown of privacy views

These results correspond to what was expected due to the survey population consisting mainly of Worcester Polytechnic Institute students. In other words, since the majority of the population was college-aged individuals, the responses received consisted mainly of people who were growing up as the Internet was developing. It is possible that because the population was exposed to the Internet at an early age, they were also exposed to the issues related to online privacy. This could be an underlying reason as to why most of the privacy views represented in the data were Privacy Fundamentalists and Privacy Pragmatists, because they were aware of the

risks following the use of the Internet, which may have influenced their concern about online privacy.

A similar result to the breakdown of privacy views can be seen in Jensen's study titled *"Self-Reports Versus Observed Behavior"*, in which each "trial" of his study resulted in over half of the respondents being categorized as Privacy Pragmatists (Jensen, 2005). The second highest represented group was Privacy Fundamentalists, followed by Privacy Unconcerned, where the percentage of Unconcerned represented in Jensen's study was 23.0%, compared to the 2.6% found within this study. One reason as to why this may have occurred is sampling bias, in which our survey population consisted mainly of college students, whereas the population in the Jensen study contained a larger variety of ages and backgrounds. However, despite this possible bias in results, the Jensen study does provide some support to our results, due to the very similar breakdown of privacy views represented in both studies.

After the survey participants were separated into groups based on privacy views, the data was further analyzed in order to determine if there was a relation between a person's privacy view and their preference towards convenience or privacy. This was done by examining the responses received to the following question:

What is more important to you, convenience or privacy?

According to the data collected (Figure 2), approximately 61.7% of the Fundamentalist responses valued privacy over convenience, whereas 51.3% of the Unconcerned group showed a slight preference toward privacy. This was not an expected characteristic of the Unconcerned group, which would have ideally shown a tendency to value convenience over privacy rather than exhibit an almost even breakdown. One reason as to why this may have occurred could be that the sample size of the Privacy Unconcerned group was too small, causing a bias in results

since the majority of the participants were Worcester Polytechnic Institute students that were mostly considered Privacy Fundamentalists and Pragmatists (Figure 9). However, despite the unexpected outcome for the Unconcerned group, the prediction that a person's privacy view correlates to their preference towards privacy was proven true. This can be observed from the difference in percentages among the privacy groups and their preference towards privacy or convenience.

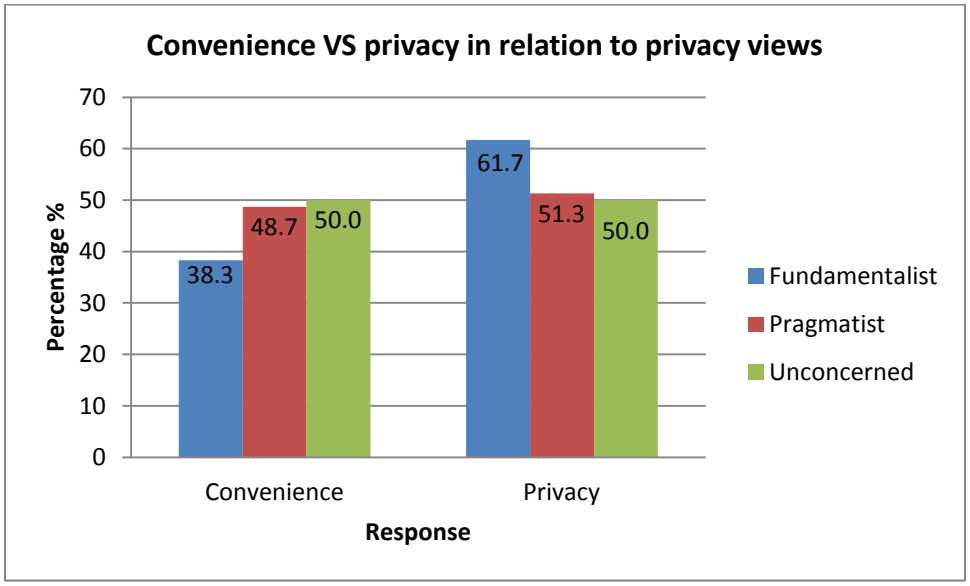

Figure 2: Convenience VS privacy based on privacy views

Additionally, the Privacy Unconcerned participants, who are expected to be carefree about privacy online, may not value convenience over privacy because it does not affect them directly. In other words, the Privacy Unconcerned group may consist of participants who generally do not care about privacy online, unless it affects them personally. This idea is supported by one of the interview subjects from this study, in which the participant registered all signs of being Privacy Unconcerned, but when asked the question of which is more important, convenience or privacy, they replied "privacy." When asked for an explanation, they elaborated on their choice by talking about the desire to keep their banking information safe to ensure their

accounts are not compromised. This provides some evidence that participants, who are considered to be Privacy Unconcerned, are not necessarily completely careless about privacy online when it comes to them personally.

Another analysis that was performed determined if educating the participant on the dangers following the use of various online services would cause them to reconsider their use of various online services based on their responses to the following question:

Do you think that being aware of the risks related to these services will change your attitude towards internet privacy and your behavior online? (Yes/No)

From the data collected (Figure 3), it can be seen that a large percentage of the survey population (across all privacy groups) claimed they would change their behavior after being informed of the risks. The data suggests that people are not intentionally practicing risky behaviors because of convenience, but are doing so because they are unaware as to the potential consequences of their actions.

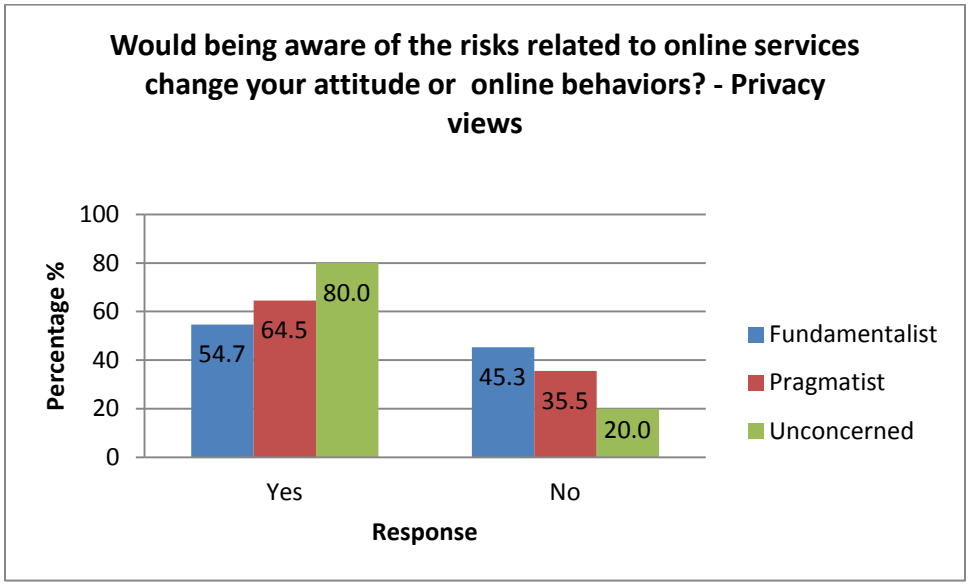

Figure 3: Changes in behavior based on privacy views

The most informing feature presented in Figure 3 is the large percentage of the Unconcerned category that claim they would change their online behavior. This strongly suggests that the reason why these participants are considered Privacy Unconcerned is because the risks following the use of the Internet are unknown to them, so they do not feel the need to be concerned with privacy. This notion however, was later disproved when a majority of the participants claimed to be aware of the risks following the use of social networking, e-commerce, and online banking (Figure 4).

The next analysis performed on the data collected determined how aware participants were about the risks associated with the online services of social networking, e-commerce, and online banking based on the responses received to the following questions:

Are you aware of the risks that come with social networking sites? (Yes/No)

Are you aware of the risks that come with E-commerce? (Yes/No)

Are you aware of the risks that come with Online Banking? (Yes/No)

As seen in Figure 4, most of the participants appeared to be aware of the risks associated with social networking, which could potentially be a result of the large number of Worcester Polytechnic Institute students that participated in the survey. In other words, since most of the participants were college-aged individuals, they grew up as social networking was being introduced online and were commonly exposed to the service. This would allow these participants to be very knowledgeable about social networking and the risks associated with its use.

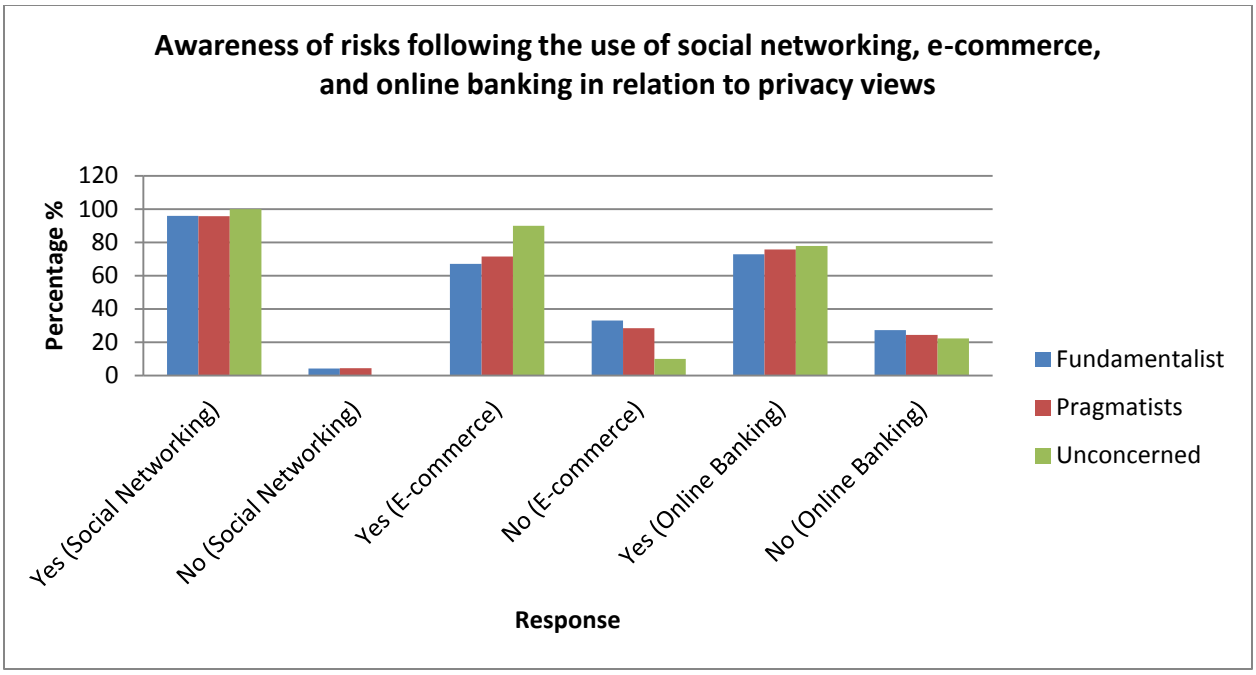

Figure 4: Awareness of risks based on privacy views

Additionally, it can be seen (Figure 4) that most people are unaware of the risks associated with the service of e-commerce. One explanation as to why a majority of the participants seem unaware of these risks is because they trust the service providers. In other words, when a person uses the service of e-commerce, they trust the company they are purchasing from and do not concern themselves with possible risks that may arise from its use. This could also apply to the service of online banking, in which participants also seem to be unaware of the risks associated with its service. This notion that people are unconcerned about privacy because they trust their information is kept confidential is supported by one of the interview subjects who claimed to do a lot of shopping online. The interview participant stated that she shopped online from companies with professional looking sites that displayed security confirmations, and expected her information to be handled confidentially and securely by the e-commerce websites she uses.

Also, according to Figures 3 and 4, it can be observed that Fundamentalists seem to be the least knowledgeable about the risks associated with the use of e-commerce and online banking. This could indicate that the actions and views of Fundamentalists come from their desire to protect their privacy, rather than their knowledge level concerning these services, which was previously believed. Conversely, the Unconcerned group seemed to be the most knowledgeable about the risks associated with the use of social networking and e-commerce. This suggests that the Unconcerned are aware of the consequences associated with the use of online services, but simply do not care about or believe themselves to be at risk.

The next analysis performed on the data determined how likely participants were to reconsider the use of various online services based on responses received to the following question:

Would you reconsider the use of any of the services previously mentioned?
Please answer for each.

	Yes	No	Maybe
Social networking			
E-commerce			
Online banking			

Although this data (Figure 5) does not exhibit any significant conclusions, it does reveal a lot of information about the difference in responses.

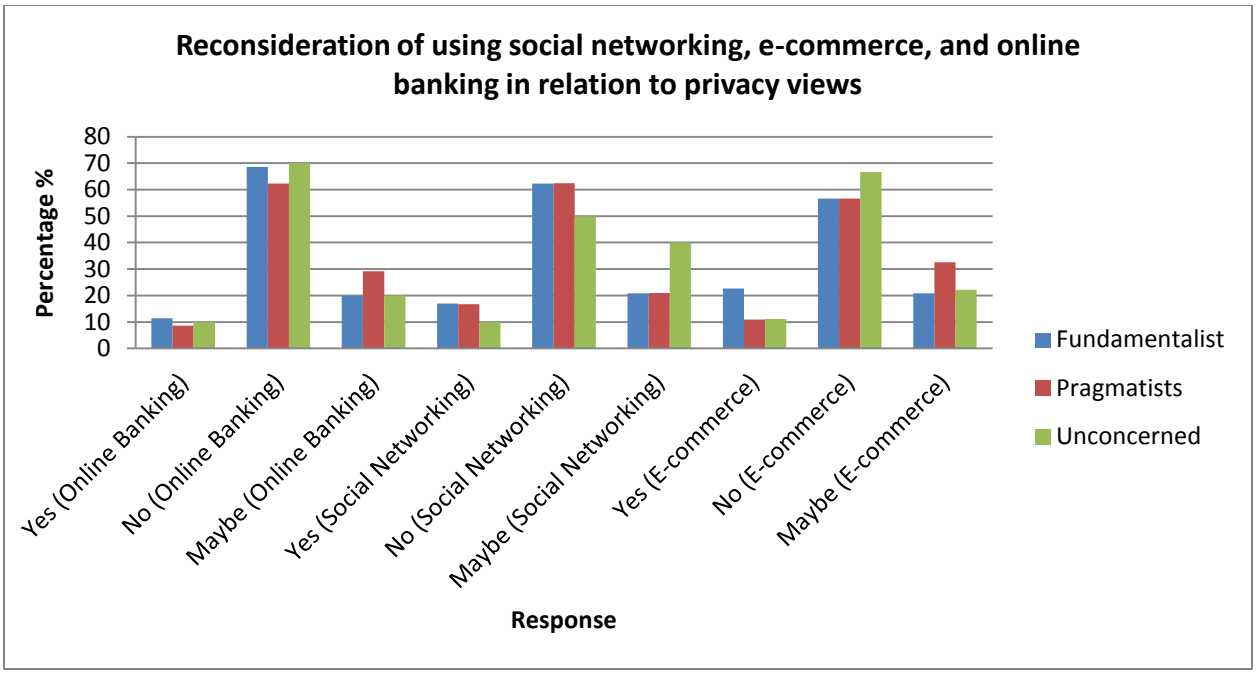

Figure 5: Reconsider use of services based on privacy views

From the data (Figures 4 and 5), it can be seen that there is a greater percentage of people claiming to be aware of the risks following the use of various online services, compared to those claiming they would reconsider the use of these services. This contradiction implies that people may want to keep their privacy protected from the risks following the use of the Internet, without needing to sacrifice the conveniences offered. This statement is supported through all of the interviews conducted, in which the subjects unanimously stated that they did not feel privacy should need to be mutually exclusive from convenience. This mindset is very reflective of the previous observation, in which people seem to be trusting of services that handle their financial information such as e-commerce or online banking.

Education and Gender Analyses

In total, there were 388 survey responses received, in which 341 (88%) were Worcester Polytechnic Institute (WPI) students and 40 (11%) were non-WPI participants. Additionally, out of the 388 responses, 200 (52%) of the participants were male and 186 (48%) were female. The

number of responses received by males was expected to be much higher than that of females due to the two-to-one gender ratio exhibited at Worcester Polytechnic Institute. However, due to this disproportion in responses based on gender, the results may exhibit bias towards female positions on the issues presented. Additionally, since the number of non-WPI participants is much less than that of Worcester Polytechnic Institute, this may indicate a bias in the results since the majority of responses received came from participants who are believed to be more knowledgeable about technology. In order to minimize the effect of these biases on the data collected, all the data analyses between Worcester Polytechnic Institute students and non-WPI participants, as well as females and males, was done in percentages rather than raw numbers.

One of the issues analyzed within this study determined if there was a correlation between how knowledgeable participants were about Internet privacy, and their attendance at Worcester Polytechnic Institute based on the responses received to the following survey question:

Please rate your knowledge about internet privacy on a scale of 1 to 5

	1	2	3	4	5	
No knowledge at all	○	○	○	○	○	Extremely knowledgeable

According to the data collected (Figure 6), it seems that non-WPI participants believe they are more knowledgeable about Internet privacy compared to Worcester Polytechnic Institute students. In total, approximately 81% of the responses received from non-WPI participants, and only 75% of the responses received from Worcester Polytechnic Institute students, believed that their knowledge level about Internet privacy rated a '3' or higher.

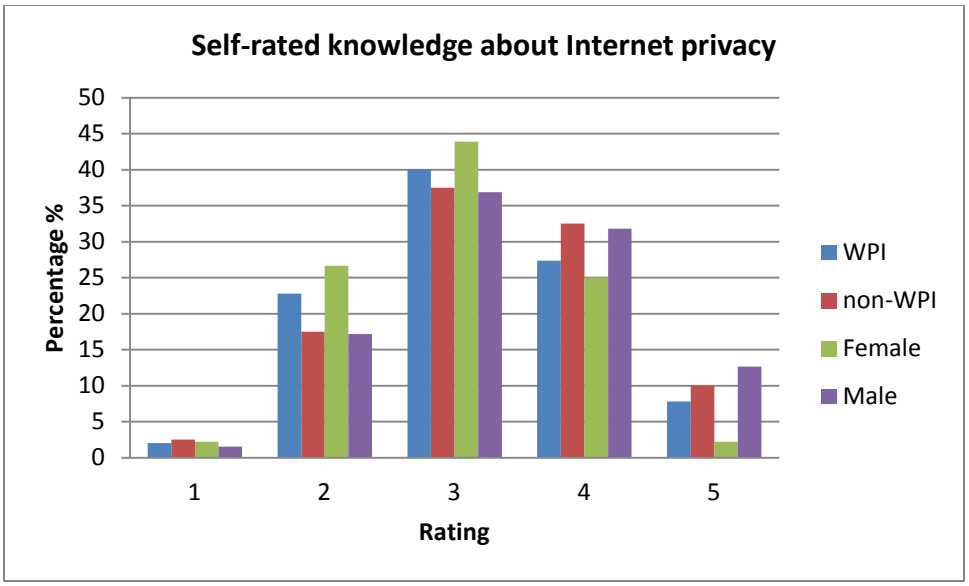

Figure 6: Internet privacy knowledge based on education and gender

These results contradict what was originally expected, which was that Worcester Polytechnic Institute students would be more knowledgeable about Internet privacy, due to their strong curriculum in technology, when compared to non-WPI participants. One explanation as to why this may have occurred is that non-WPI participants believe that they are very knowledgeable about Internet privacy, when in actuality they are not as knowledgeable as they perceive. A similar result can be seen in Jensen's study, in which respondents perceived their knowledge to be higher than it really was. This concept was supported in Jensen's study when a knowledge test was administered to the respondents, which resulted in their tested knowledge being less than their perceived knowledge. Although our study did not test participants to determine if there was a difference between their perceived and actual knowledge, it is a possibility that non-WPI participants tend to exaggerate their actual knowledge level about Internet privacy.

A similar issue that was analyzed determined if gender had an effect on a person's knowledge about Internet privacy. According to Figure 6, approximately 82% of male

respondents and 71% of female respondents believed that their knowledge level about Internet privacy rates a '3' or higher. This may imply that males tend to believe they are more knowledgeable about Internet privacy than females. One explanation as to why males may tend to believe they are more knowledgeable about Internet privacy than females is because most of the participants that responded to the survey were Worcester Polytechnic Institute students. Additionally, a higher proportion of males to females that attend Worcester Polytechnic Institute tend to major in Electrical and Computer Engineering or Computer Science, whereas a higher proportion of females to males tend to major in Biology, Chemistry, Biomedical Engineering, and Chemical Engineering. This distribution among majors at Worcester Polytechnic Institute, as well as the fact that there are more male engineers in society than females, could be plausible reasons as to why males are more familiar with technology and claim to be more knowledgeable about Internet privacy compared to females.

Another topic of analysis within this study was to determine the relation between how knowledgeable people are about protecting themselves online, and their attendance at Worcester Polytechnic Institute based on the responses received from the following survey question:

Please rate your knowledge on protecting yourself from online threats on a scale of 1 to 5

	1	2	3	4	5	
No knowledge at all	○	○	○	○	○	Extremely knowledgeable

According to the data (Figure 7), as the rating of knowledge increases, the percentage of Worcester Polytechnic Institute students' responses also increases until it reaches a peak at '4.' Although the number of Worcester Polytechnic Institute responses seems to rise as the rating increases, the percentage of Worcester Polytechnic Institute students who rated themselves at least a '3' or higher on the scale is less than the percentage of non-WPI participants. In total,

approximately 84% of the responses received from non-WPI participants, and only 77% of the responses received from Worcester Polytechnic Institute students, believed that their knowledge level about protecting themselves from online threats rated a '3' or higher.

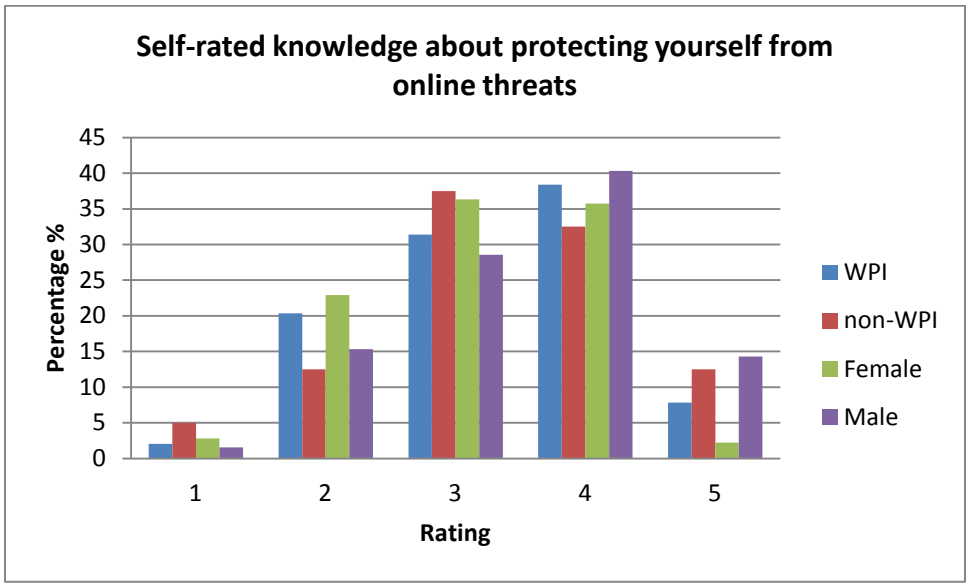

Figure 7: Protection knowledge based on education and gender

Again, these results contradict what was originally expected, which was that Worcester Polytechnic Institute students would be more knowledgeable about protecting themselves online compared to non-WPI participants. One reason as to why this may have occurred could be that again, non-WPI participants may believe that they are more knowledgeable about protecting themselves from online threats, when in actuality they are not as knowledgeable as they perceive. However, since our study did not test participants to determine if there was a difference between their perceived and actual knowledge in protection from online threats, there is no way to provide evidence as to why this may have occurred.

Similarly, the data collected from the survey was also analyzed to determine if gender had an effect on a persons' knowledge about protecting himself or herself from online threats. As seen in Figure 7, approximately 83% of responses received from male participants and 74% of

responses received from female participants believed that their knowledge level about protecting themselves from online threats rated a '3' or higher. In other words, it seems that males tend to believe they are more knowledgeable about protecting themselves from online threats compared to females. Again, this could be a result of males being more familiar and surrounded by technological advances in society and school, since there are fewer females who study technological and engineering studies.

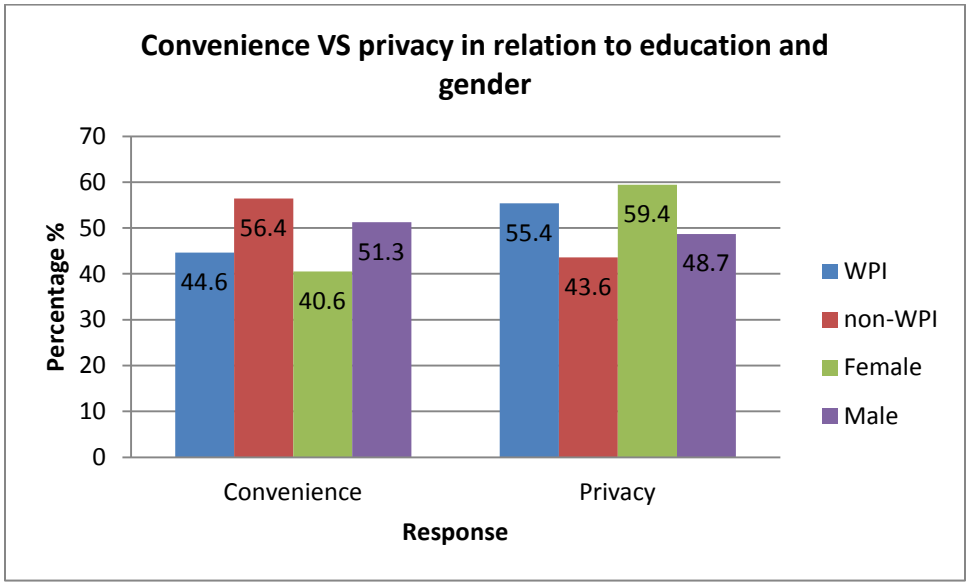

Figure 8: Convenience VS privacy based on education and gender

The data collected from the survey responses were also analyzed in order to determine if a person's attendance at Worcester Polytechnic Institute would cause them to value convenience over privacy. As seen in Figure 8, 55.4% of Worcester Polytechnic Institute students valued privacy more than convenience, whereas 43.6% of non-WPI participants valued privacy over convenience. One explanation as to why this may have occurred is that, since Worcester Polytechnic Institute students are familiar with technology as a result of the curriculum provided, they may be more aware of the risks that follow the use of the Internet. This may then imply that Worcester Polytechnic Institute students tend to value privacy more than convenience because

they are aware of the possible consequences that may result from using the Internet, whereas non-WPI participants may tend to value convenience over privacy since they are not aware of these risks or consequences.

A similar issue that was analyzed determined if gender had an effect on whether a person would value convenience over privacy. According to the collected data (Figure 8), approximately 59.4% of female participants preferred privacy over convenience, whereas 48.7% of male participants preferred privacy more than convenience. From this analysis, it would seem that males tend to value convenience more, whereas females tend to value privacy. If the prior analysis about males being more knowledgeable about protecting themselves from online threats is true, then it is possible that they may tend to value convenience more than privacy, since they are already knowledgeable in protecting themselves online. In other words, males may feel that they protect themselves adequately online and can benefit from the conveniences offered by the Internet without putting their privacy at risk, whereas females are not as knowledgeable and value their privacy more. Females may value their privacy more than convenience because although they are unaware of the risks relating to these specific online services, they may be aware that privacy risks exist online. It was concluded from the survey results that approximately 6.3% more females than males were not aware of the risks following the use of social networking. Additionally, 8.5% and 7% more female respondents stated they were unaware of the risks following the use of e-commerce and online banking when compared to male respondents.

The next issue analyzed within this study determined if a person's attendance at Worcester Polytechnic Institute would affect their privacy views or their concern for privacy online. Depending on the responses the participants provided, they were then categorized as

Privacy Fundamentalist (highest concern for privacy), Pragmatist (intermediate concern for privacy), or Unconcerned (least concern for privacy). After each participant was categorized, we were then able to determine if there was a correlation between a person's attendance at Worcester Polytechnic Institute and their concern for privacy. As seen in Figure 9, 98% of Worcester Polytechnic Institute students 93% of non-WPI participants were considered either Privacy Fundamentalists or Privacy Pragmatists, whereas only 2% of Worcester Polytechnic Institute students and 8% of non-WPI participants were considered Privacy Unconcerned.

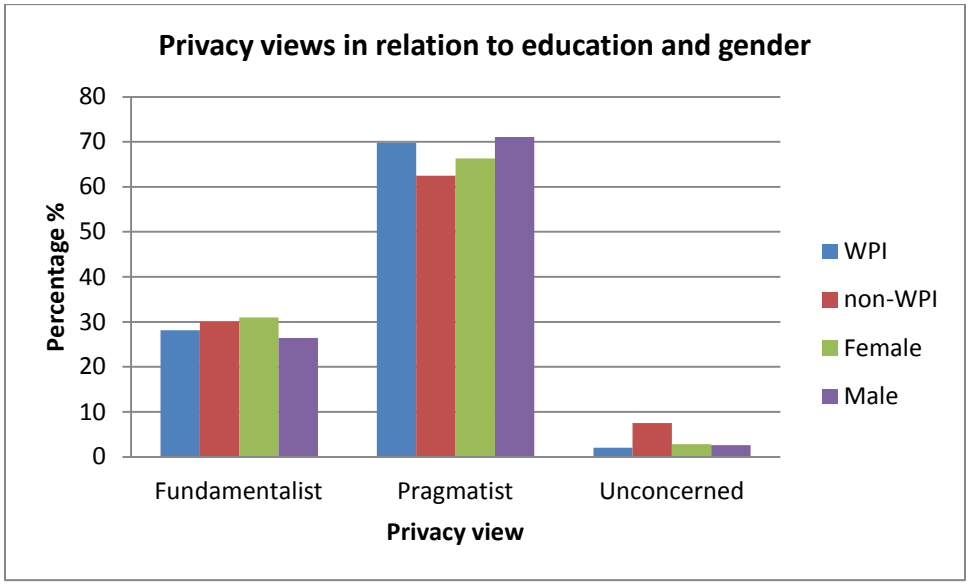

Figure 9: Privacy views based on education and gender

One explanation as to why this breakdown among privacy views may have occurred is that since Worcester Polytechnic Institute students are more familiar with technology, they may be more aware of the risks that follow the use of the Internet compared to non-WPI participants. Therefore, it is possible that because Worcester Polytechnic Institute students are aware of the possible risks that follow the use of the Internet, they would be concerned about privacy online and how it is protected and handled by online services. However, since our study did not

question participants as to why they might be concerned about privacy, there is no way to provide evidence as to why this may have occurred.

A similar issue that was analyzed determined if gender had an effect on a person's privacy views or concern for privacy online. According to the collected data (Figure 9), approximately 26% of male participants and 31% of female participants were considered Privacy Fundamentalists. Additionally, 71% of males and 66% of females were determined Privacy Pragmatists, whereas 3% of male and female participants were considered Privacy Unconcerned. From this analysis, it would seem that females are slightly more concerned about privacy online compared to males.

Again, if the prior analysis about males being more knowledgeable about Internet privacy and protecting themselves from online threats is true, then it is possible that they may not be concerned about privacy, since they are already knowledgeable on the topic and how to protect themselves. As a result, males may feel that they know enough to protect their privacy sufficiently online and are no longer concerned, whereas females may not be as knowledgeable and therefore are concerned about their privacy online. Although there is no significant data to support this inference, this could be a plausible reason as to why females may be more concerned about privacy than males.

The data collected from the survey responses were also analyzed to determine if gender had an effect on a person's willingness to change their online behaviors as a result of being informed about the risks that follow the use of social networking, e-commerce, and online banking. From the data collected, it was determined that on average, 46% of females stated that they would consider changing their attitude and online behaviors, whereas 67% of males would not reconsider their attitudes toward or use of these online services. This may imply that females

are more willing to change their online behaviors as a result of being informed of the risks following the use of these online services, whereas males are less likely to change their online behaviors because they were already aware of these risks. In other words, males may have already taken precautions to protect their privacy online since they are already aware of the risks following these services, resulting in no need to change their online behavior. Additionally, since females may not be as aware of these risks compared to males, as previously mentioned, they may not have taken actions to ensure the protection of their privacy and are willing to change their behavior to increase their privacy protection online.

Hours Spent Online Analysis

In order to explore if the amount of time spent online affects a user's knowledge, beliefs, or practices regarding Internet Privacy, the data collected was sorted based on the amount of time participants claimed to spend online determined from the response received to the following question:

How long do you use the internet for non-work and non-academic reasons each day

- 1 hour or less
- More than 1 hour, less than 4 hours
- More than 4 hours, less than 7 hours
- More than 7 hours

This resulted in four different groups: 1 hour or less, between 1 and 4 hours, between 4 and 7 hours, and more than 7 hours. As seen in Figure 10, 58% of the survey participants claimed to spend between 1 and 4 hours online each day, whereas 26% claimed to spend between 4 and 7 hours. Additionally, 9% of the participants stated they spend more than 7 hours online each day, and 7% stated they spend 1 hour or less.

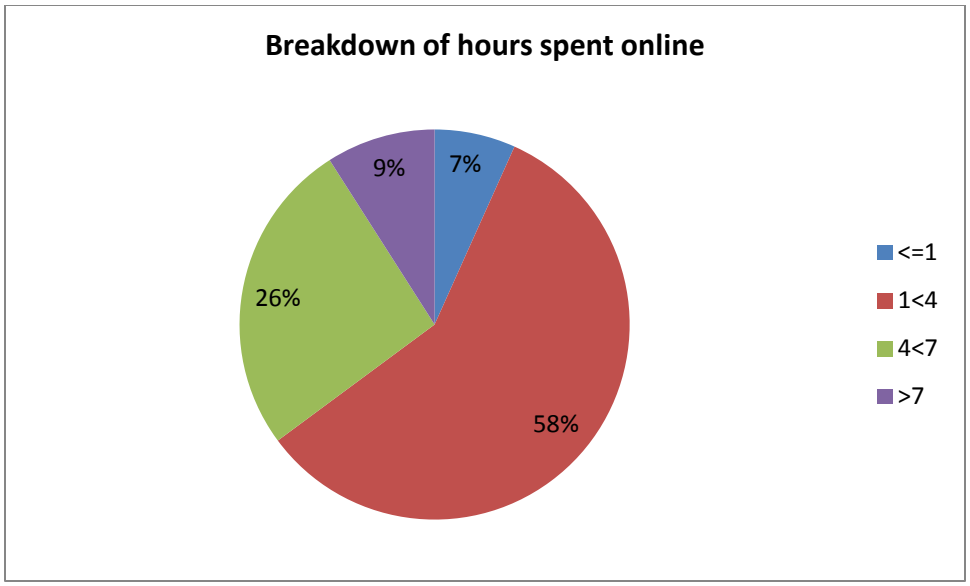

Figure 10: Breakdown of hours spent online

Once the participants were sorted based on the amount of time they spent online, the data was further analyzed to determine how knowledgeable participants were about Internet Privacy and protecting themselves from online threats. As seen in Figure 11, there is an increasing trend in the self-rated knowledge about Internet Privacy and protection from online threats as people spend more time using the Internet. This supports the original hypothesis that the more time a person spends online, they more knowledgeable they are about Internet privacy and protecting themselves online.

The data collected from the survey was then further analyzed (Figure 12) to determine if there was a correlation between how many hours a person spends online and which protective software the participant uses to protect themselves from online threats. Although there is no distinct trend seen in the reported use of antivirus software, it is interesting that the use of ad-blockers and anti-malware software is more frequent as users spend more time online. Ad-blockers and anti-malware software protects users from undesirable online advertising and malicious attacks.

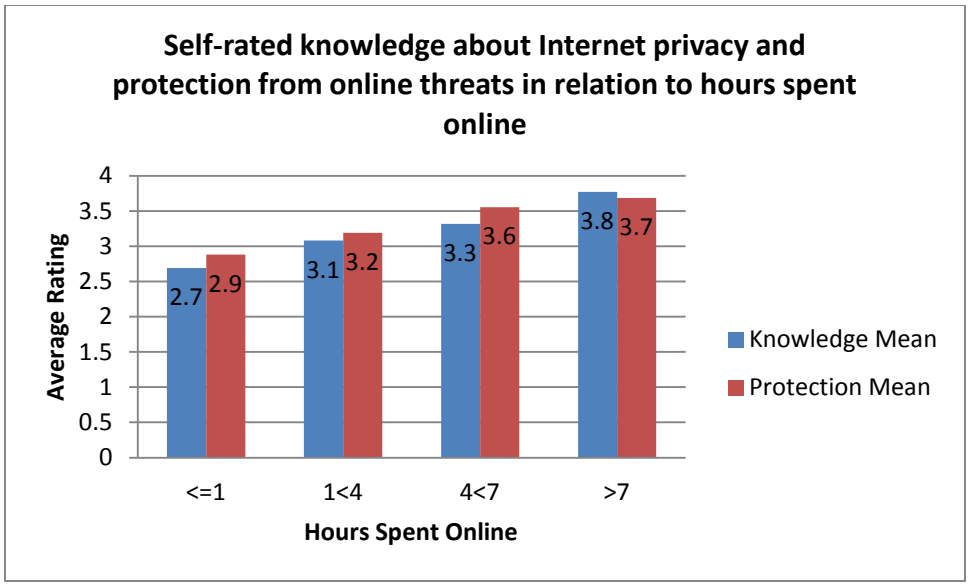

Figure 11: Knowledge and protection based on hours spent online

The increase in use of these software support the suggestion that people gain some amount of knowledge about protecting themselves from online threats as they spend more time online. This could either be a result from previous experiences when dealing with these advertisements or malicious attacks, or other sources of information.

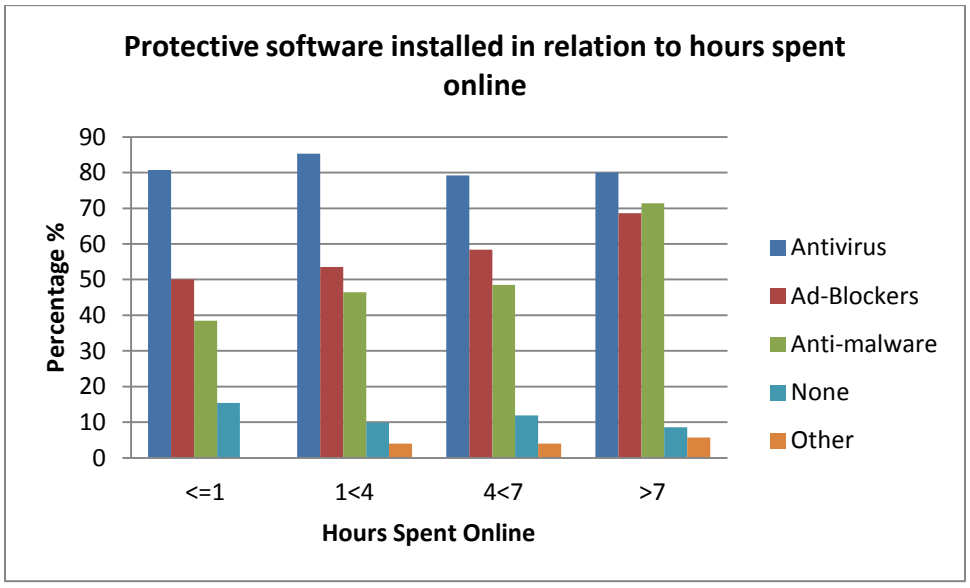

Figure 12: Protective software based on hours spent online

Additionally, the data collected from the survey was analyzed in order to determine if there was a relation between the numbers of services a person uses and the amount of time they spend online based on the responses received from the following survey question:

Which of the following protective software do you have installed on your computer
Check all that apply.

- ☐ Antivirus software
- ☐ Anti-malware software
- ☐ Ad-Blockers
- ☐ None
- ☐ Other:

From the results gathered, there seems to be a positive correlation between the number of services people use and the amount of time they spend online. This may suggest that these variables are directly related. Similarly, further data analysis suggested that the more time a person spends online, the higher he or she rated the convenience level of the online services they used. There also seems to be a ceiling, where although antivirus software is the most commonly used piece of protective software, 10% of Internet users do not use this piece of software, regardless of the time they spend online.

The next point of analysis for this study was to determine if informing a person about the risks associated with various online services would lead them to change their attitude toward or use of the services. Figure 13 shows that the less time a person spends online, the more likely they are to change their attitude towards Internet Privacy and their online behavior. This suggests that the less time a person spends online, the less knowledgeable they are about the risks following the use of the Internet. This would make them more likely to change their habits online as they learn about these risks that they were unaware of before, in order to better protect their privacy online.

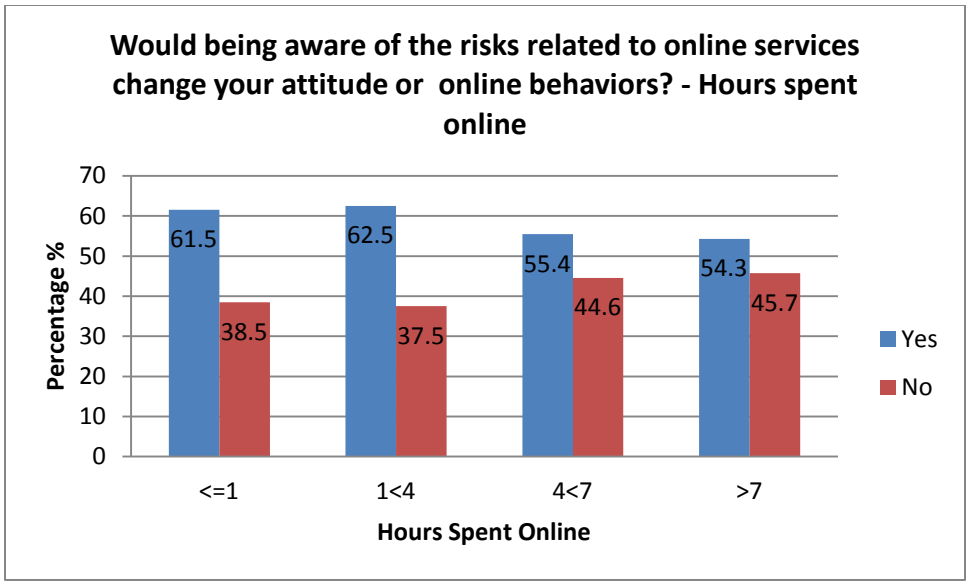

Figure 13: Changes in behavior based on hours spent online

On the other hand, those users who spend a lot of time online are less likely to change their attitude because of two possible reasons. They could have already been aware of the risks and took prior precautions to protect their privacy, or they value the conveniences offered by these services so greatly, that they underestimate the consequences following the risks that arise online.

Another point of analysis within this study was to determine if the amount of time a person spent online would affect their concern about privacy based on the responses received to the following question:

Please rate your concern about your privacy when using the Internet on a scale of 1 to 5

	1	2	3	4	5	
No concern at all	○	○	○	○	○	Extremely concerned

According to the results (Figure 14), there seems to be a positive correlation between the amount of time a person spends online and their concern for privacy. This may suggest that the

more time a person spends online, the more knowledgeable they become about the risks associated with the use of the Internet. This may imply that as users spend more time online and are becoming more knowledgeable about the issues dealing with Internet privacy, the more concerned they are about the Internet. Although there is no significant data to support this claim, it is a possible explanation as to the trend that can be seen in Figure 14.

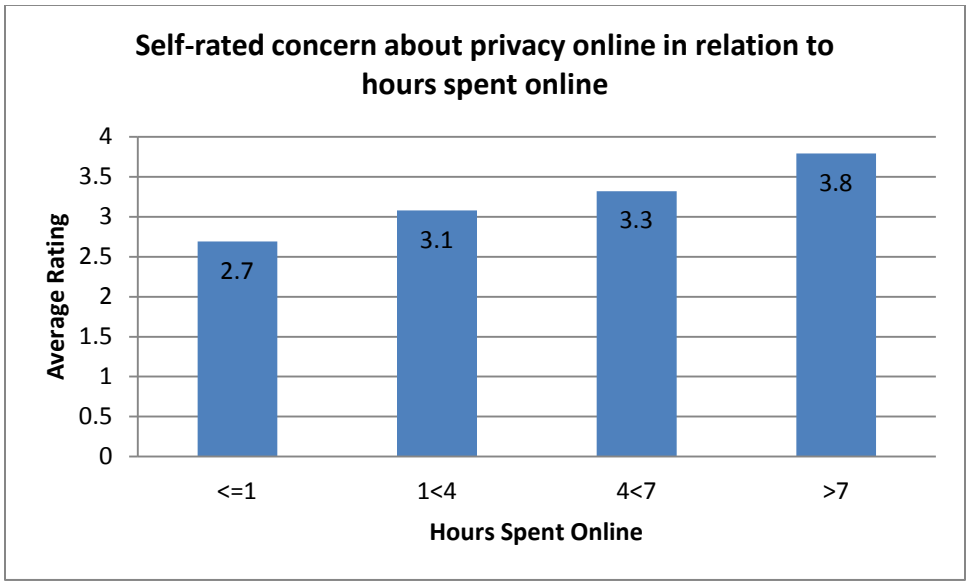

Figure 14: Privacy concern based on hours spent online

The data collected from the survey was then analyzed in order to determine if the amount of time spent online influences a person's preference toward convenience or privacy. As seen in Figure 15, as the number of hours the participants spend online increases, the more they prefer convenience over privacy. One explanation as to why this may have occurred could be due to the fact that if a person feels more confident in their knowledge about protecting their privacy online, as a result of spending a lot of time online, they would value convenience because they are already protected online. Another explanation could be that as the participants spend more time online, the more likely they are to underestimate or forget about the risks that arise online as a result of benefiting from the conveniences offered. This may also explain why the group of

users who spend 1 hour or less online, tend to value privacy more than convenience. In which case, the users might not be aware of the risks they are exposed to and would value their privacy more since they are unprotected online. Although these are plausible reasons as to why participants seem to value convenience as they spend more time online, there is no evidence to support these inferences.

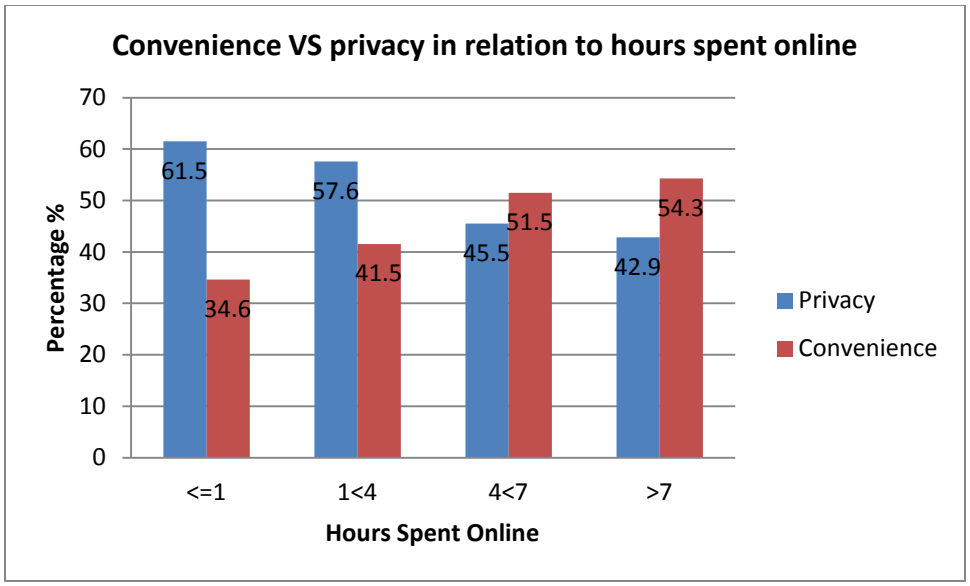

Figure 15: Convenience VS privacy based on hours online

The final analysis performed on the data collected determined if the was a relation between the amount of hours participants spent online, and their use of various online services based on the response received to the following survey question:

On a scale of 1 to 5, how much personal information do you think you share with your social networking site

	1	2	3	4	5	
Very little information	○	○	○	○	○	A lot of information

Although no significant data was found within the services of e-commerce, and online banking, it was determined that there was a correlation between the amount of hours a person spent online and the amount of information they shared on social networking sites.

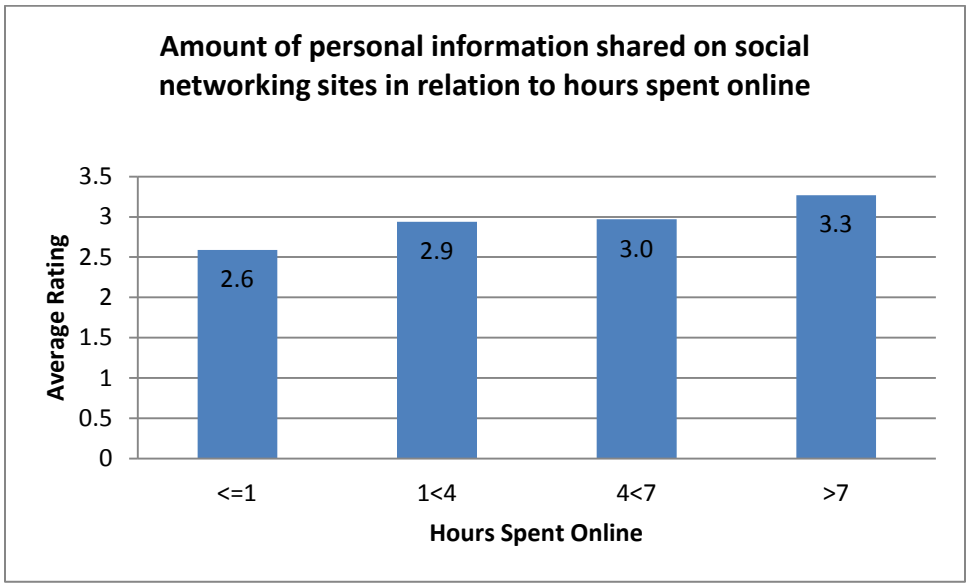

Figure 16: Information shared based on hours spent online

The results shown in Figure 16 suggest that users who spend more time online tend to share more information on their social networking accounts. One plausible explanation as to why this trend may have occurred could be due to the "addictive" nature surrounding the use of social networking, in which many teenagers and young adults use the service.

4.2 INTERVIEW ANALYSIS

In total, there were 4 interviews conducted, in which all the participants were female Worcester Polytechnic Institute (WPI) students. Out of the 4 interviews, 1 was considered a Privacy Fundamentalist, 1 was Privacy Unconcerned, and 2 were Privacy Pragmatists.

During the interview process, each participant was asked if they valued convenience more than privacy, in which all of the participants replied that they did not believe convenience and privacy should be conflicting factors when using online services. In other words, the

participants believed that the conveniences offered by the Internet should not cost them their privacy. They then elaborated on their response by stating that they felt their information should be handled in a manner that would ensure it was kept confidential while also being able to benefit from the conveniences offered. This mentality provides some insight as to why Internet users may use online services that put their privacy at risk, as seen in the results gathered from the survey.

Additionally, the interviews conducted provided an explanation as to why Internet users may want to use the online services of social networking, e-commerce, and online banking. The results were very consistent in relation to social networking, in which all the participants expressed the desire to keep in contact with their friends by using the service of social networking. Each interview participant stated that they had friends from different states or countries and that social networking provided them with the convenience of easily keeping in contact with each other. These responses support the data collected from the survey population, in which most of the participants were college-aged individuals, because it would explain why most of the survey participants used the social networking service.

Three of the interview participants also claimed to moderate the amount of information visible on their social networking sites by restricting who could see their information posted on their account. The Fundamentalist then elaborated by stating she also altered her name so it could not be readily searchable online, whereas the Unconcerned participant was not troubled about who could see their social networking profile since they did not share any personal information.

In terms of why participants may want to use the service of e-commerce, all the interview participants stated that they used the service since it was the most convenient way for them to shop. They elaborated by stating they all did not have a car on campus and that there are not a lot

of stores within walking distance of Worcester Polytechnic Institute. This situation provides an explanation as to why the majority of survey participants, who were Worcester Polytechnic Institute students, stated they would not reconsider the use of e-commerce after being aware of the associated risks.

The interview participants also mentioned that they were cautious with e-commerce sites in order to ensure the protection of their personal information. This was done by using only e-commerce sites with a security confirmation symbol on the website that would guarantee the participants' personal information was not at risk. These interview responses provide some support to the interferences made from the survey, in which participants trust the online service provider to keep their information confidential, and as a result do not concern themselves with the possible risks that may arise. Additionally, the interview participants had a similar opinion about the service of online banking, in which they did not see it as a big risk to their privacy because they trusted that their banks would keep their information confidential.

When the participants were asked about how concerned they were about privacy, they seemed to be very knowledgeable, but also very concerned, about the risks following the use of social networking. On the other hand, the participants seemed to be unaware of the risks associated with the use of e-commerce and online banking. This reinforces the results found in the survey, in which the participants within this study seem to practice risky behaviors due to their lack of knowledge related to the consequences and risks that follow the use of the Internet.

The participants were then asked if they believed these online services compromised, or could compromise, their privacy. There were slight discrepancies in the responses received, in which three of the interview participants stated that they felt the service of social networking could compromise their privacy. However, despite their belief, these participants continued to

use the service of social networking because they felt that their security settings were strong enough to protect their personal information. On the other hand, the other interview participant, who was considered a Privacy Fundamentalist, believed that social networking could compromise anyone's privacy despite their level of security settings. Although this interview participant expressed strong concerns about privacy within the service of social networking, she also continued to use the service because she believed there was no personal information on her profile capable of compromising her privacy.

The other slight inconsistency was observed within the service of online banking, specifically related to the use of mobile devices to check bank accounts. In this case, the Fundamentalist understood the risks that arose when using a mobile device to check their bank accounts. From this understanding, they then elaborated by stating they do not use mobile devices to check their accounts because the level of protection offered for mobile platforms is not strong enough to protect a person's privacy.

In contrast, the other interview participants stated that they were unaware of the risks and consequences that would arise from using a mobile device to check their financial activity. The Unconcerned participant then specified that she does check her balance through a mobile device, but she was also unaware of the risks following the use of online banking in general. After informing her of the risks, she then stated that she would reconsider the use of her mobile device. This provides some evidence that while Privacy Unconcerned individuals may claim to be aware of the risks following the use of online services, they may not actually be aware of these risks or following consequences.

Overall the interview responses were consistent with the information gathered from the online survey and provided some insight as to the trends observed in the survey. Generally it was

seen that people do not believe convenience and privacy should be mutually exclusive when dealing with online services. The interviews also suggested that informing a person about the risks associated with the Internet might cause them to reconsider their use of online services.

5. CONCLUSIONS

In conclusion, the results gathered from the online survey and interviews were very informative as to the opinions and habits expressed by Internet users. From the survey, it was determined that the majority of the survey population could be categorized as Privacy Pragmatists. It was also concluded that female participants and Worcester Polytechnic Institute students tend to value privacy over convenience, whereas the inverse was found in male and non-WPI participants. The final conclusion drawn from the survey determined that as users spend more time online, the more knowledgeable they are about Internet privacy and protecting themselves online.

5.1 PRIVACY ISSUES

Advances in various communication fields, such as the Internet, have had a great impact on the way people share their personal information. Online service providers, such as Google and Facebook, are gradually changing their privacy policies in order to allow them to collect more information about users with the intention of increasing the conveniences offered by their services. As a result, users are forced to choose between risking their privacy and discontinuing the use of these services. Since the number of people that use these services is increasing, it seems logical to question whether a privacy problem arises with the changing state of the Internet.

In the case of Google, the company is declaring that it will collect data on its users in order to improve the quality of its services. Since Google is changing its privacy policies, current and future users of their services will have to consent to new terms of service agreements in order to use their services. This has caused some users to become concerned for their privacy, whereas other users seem to be unaffected. One reason as to why some Internet users may not be

concerned about these privacy issues is that they become so dependent on these services that they are willing to sacrifice their privacy for them. On the other hand, some of the users that oppose these changes are concerned that Google may collect their data for one purpose, but also use it for another. Additionally, the Federal Trade Commission (FTC) has previously ruled that Google violated its privacy policy when it used information collected from Gmail for another purpose – Google Buzz – without obtaining permission from consumers in advance (Federal Trade Commission, 2011).

Consumer and privacy advocates are worried that services like Google and Facebook already collect a lot of information about their users, and are strongly against policy changes. Additionally, the Electronic Privacy Information Center (EPIC) is suing the Federal Trade Commission for failing to protect consumers' privacy by not taking action against the pending policy changes for Google (EPIC, 2012). This growing interest in Internet privacy issues has also affected the Obama administration, which has recently announced its support for an Internet privacy bill of rights (Office of the Press Secretary, 2012). This bill would set Internet privacy standards for all major Internet companies such as Google, Facebook, and the Microsoft Corporation. This bill would also provide consumers with access to the information companies have collected on them, and allow them to set restrictions as to how their information is used. This pending Internet privacy bill of rights will also allow Internet users the option of deleting the information that companies have collected on them.

However, despite all these changes in privacy policies, only a small number of consumers seem to be seriously concerned with what is happening online. One reason why consumers may not be concerned is because they do not completely understand how their privacy may be at risk.

It is important for Internet users to understand what privacy policies are changing in order for them to adequately protect their privacy online.

While the future is unknown and it is impossible to determine the impact these changes will have on our lives, history has shown that innovations in technology sometimes bring fear into peoples' lives. One example of such an event occurred about a century ago, when President Roosevelt decided to ban the use of Kodak cameras in Washington DC parks because he was worried that this new invention would invade peoples' privacy. Although this ban did not last very long, and even though there was a concern for peoples' privacy, cameras are now a part of our daily lives.

As a result, it is difficult to determine which privacy issues today will still remain a problem in the future, and which changes in privacy policies will create more privacy issues. Therefore it is important to make sure Internet users are informed about the risks that may follow the use of various online services, in order to protect their privacy. It is also very important for lawmakers to find a solution that guarantees consumer protection with the Internet's continual economic growth.

5.2 ASSESMENT OF STUDY

Overall, the developed survey seemed to be effective in determining what factors affect a participant's knowledge level and online behaviors. There were some issues, however, when interpreting the following question included in the survey:

Do you think that being aware of the risks related to these services will change your attitude towards Internet privacy and your behavior online? (Yes/No)

The "risks" referred to in this question caused some participants to misinterpret it as new risks related to online services. In other words, the participants believed they were being asked the following question:

Do you think that <u>becoming aware of new risks</u> related to these services will change your attitude towards Internet privacy and your behavior online? (Yes/No)

However, the term "risks" in the actual question referred to risks that the participants may have already known, as well as those risks mentioned in the developed survey. Therefore, the question should be rephrased to ask the following:

Do you think that <u>the risks related to these services (the risks mentioned in this survey and the risks that you are already aware of)</u> will change your attitude towards Internet privacy and your behavior online? (Yes/No)

5.3 AREAS FOR FURTHER RESEARCH

Although this study examined the effect of various factors on a person's knowledge level and online behaviors relating to privacy, there are many other areas for research relating to Internet privacy. One example is to determine if there exists a difference between a person's perceived and actual knowledge, relating to the topics of Internet privacy or their ability to protect themselves online. This could be done by administering a knowledge test to participants, in order to verify how knowledgeable they are about these topics.

Another potential area of research could be to expand this current study to apply to a wider variety of online services, such as online gaming or file sharing services. This would determine how aware online users are about risks associated with various online services, and if they are more likely to reconsider using certain services compared to others. Additionally, another topic for further research could be to determine the differing characteristics among privacy views (Fundamentalist, Pragmatist, and Unconcerned). This would examine the effect of

a person's privacy view on opinions about privacy, as well as their online behaviors. This area of research could also determine the validity of how participants may be categorized based on their privacy views.

APPENDIX A

Internet Privacy IQP 2011-2012
Participation in this survey is entirely voluntary. You may skip any question if you do not feel comfortable providing an answer for it. Results from this survey will remain completely anonymous. Thank you for taking the time to fill out this survey, your response is greatly appreciated.

Please choose the following that best describes your age

- 15-20
- 21-25
- 26-31
- 32-37
- 38-43+

Please choose the following that best describes your race

- White/Caucasian
- African American
- American Indian or Alaska Native
- Asian
- Other:

Please indicate your gender

- Male
- Female

How long do you use the Internet for non-work and non-academic reasons each day

- 1 hour or less
- More than 1 hour, less than 4 hours
- More than 4 hours, less than 7 hours
- More than 7 hours

Highest level of education completed

- Some High School (No Diploma or GED)
- High School (Diploma or GED received)
- Some College
- Associates Degree
- Bachelor's Degree
- Master's Degree or Higher

How did you find out about this survey

- Worcester Polytechnic Institute Email
- Non-WPI University Email
- Social Networking Site (Facebook, Twitter, Tumblr)
- Other:

Please rate your knowledge about internet privacy on a scale of 1 to 5

	1	2	3	4	5	
No knowledge at all						Extremely knowledgeable

Please rate your knowledge on protecting yourself from online threats on a scale of 1 to 5

	1	2	3	4	5	
No knowledge at all						Extremely knowledgeable

Select all of the following factors you think make an online service (such as social networking, banking, or shopping) most desirable

- Popularity
- Visible confirmation of site security
- Site appearance (such as layout, design, aesthetics)
- Price of item or service
- Other:

Here are some statements about the internet. Do you agree strongly, agree somewhat, disagree somewhat, or disagree strongly.
Please answer for each statement.

	Strongly disagree	Somewhat disagree	Somewhat agree	Strongly agree
The providers of on-line services should be able to track the places users go on the Internet in order to send these users targeted marketing offers.	○	○	○	○
Consumers have lost all control over how personal information is collected and used by companies.	○	○	○	○
Most businesses handle the personal information they collect about consumers in a proper and confidential way.	○	○	○	○
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	○	○	○	○

Which of the following protective software do you have installed on your computer
Check all that apply.

- ☐ Antivirus software
- ☐ Anti-malware software
- ☐ Ad-Blockers
- ☐ None
- ☐ Other: _____

Do you know what Internet privacy is?

- ○ Yes
- ○ No

Please proceed to READ the following definition of Internet privacy, before continuing:

Internet privacy, within this survey, is defined as the implicit right of an individual to be able to control their degree of exposure, in regards to their information, when using the Internet. In other words, Internet privacy is the right of a person to control his or her information and how it is shared, over the Internet.

Please rate your concern about your privacy when using the Internet on a scale of 1 to 5

	1	2	3	4	5	
No concern at all	○	○	○	○	○	Extremely concerned

Please proceed to READ the following definition of convenience before continuing:

A convenience, within this survey, is defined as an online tool that allows users to complete a task with little effort. For example, e-mail may be considered a convenience because it allows users to communicate with others through the Internet in a faster method compared to the mailing of letters.

What is more important to you, convenience or privacy?

- ○ Convenience
- ○ Privacy

Do you have an account on a social networking site?

- ○ Yes
- ○ No

Please indicate which social networking sites you use below
Check all that apply.

- ☐ Facebook
- ☐ Google+
- ☐ Myspace
- ☐ Twitter
- ☐ LinkedIn
- ☐ Other: _____

On a scale of 1 to 5, how much personal information do you think you share with your social networking site

	1	2	3	4	5	
Very little information	○	○	○	○	○	A lot of information

On a scale of 1 to 5, how convenient do you think social networks are for you

	1	2	3	4	5	
Not convenient at all	○	○	○	○	○	Extremely convenient

On a scale of 1 to 5, how strong do you think your privacy settings are on your social networking site

	1	2	3	4	5	
Very weak	○	○	○	○	○	Very strong

Which of the following pieces of personal information have you made public (posted) through any social networking site
Check all that apply.

- ☐ Real name
- ☐ Email
- ☐ Relationship status
- ☐ Sexual orientation
- ☐ Address
- ☐ Photos
- ☐ Telephone number
- ☐ Birthdate
- ☐ Job
- ☐ Other: _____

Please proceed to READ the following definition of a risk before continuing:

A risk, within this survey, is defined as the possibility that an action or activity online will lead to an undesirable outcome. For example, if the action of a picture being posted online of someone that was of an unprofessional nature (such as nudity or intoxication due to the consumption of alcohol) was later seen by a potential employer. It could lead the undesirable outcome of the person losing a job.

Are you aware of the risks that come with social networking sites?

- Yes
- No

Please READ the following short paragraph that describes the most recent risks social networking sites have been related to:

Privacy settings, policies, and the amount of information shared, define the degree to which a user's privacy is invaded in social networks. Exposure of personal information to a wider range of people, tagging (the act of associating a person with an event or photo, with or without the consent of the person), and fake profiles (in which a person pretends to be someone they are not), are all risks that the user of a social network is vulnerable to. Social networks observe and remember people's clicks, activities and interests, because having this detailed information for a vast amount of people makes them very valuable to advertisers. Facebook's "Like" button that is embedded on other sites, has been found to notify Facebook that a person visited those sites even when he or she doesn't click on the button. One example of this is, if you logged in to Facebook once in the past month, and are reading an article on cnn.com, Facebook knows. As Internet giants Facebook and Google race to expand their facial-recognition abilities, researchers at Carnegie Mellon University in Pittsburgh successfully identified about one-third of the people they tested, using their public profile pictures and a powerful facial-recognition technology. They also found that about 27% of the time, they could correctly predict the first five digits of their Social Security numbers using data taken from Facebook profiles of the subjects they identified.

Do you do any of your shopping online?

- Yes
- No

How many times did you buy goods online last month?

- 0 - 1
- 2 - 4
- 5+

On a scale of 1 to 5, how convenient do you think e-commerce is for you

	1	2	3	4	5	
Not convenient at all	○	○	○	○	○	Extremely convenient

Which of the following methods do you use to pay for items online

- ☐ Credit/Debit card
- ☐ Paypal
- ☐ E-check
- ☐ Bank account
- ☐ Other: _____

Do you make a practice of reading the terms of service before completing an e-commerce transaction?

- ○ Yes
- ○ No

Are you aware of the risks that come with e-commerce?

- ○ Yes
- ○ No

Please READ the following short paragraph that describes the most recent risks e-commerce has been related to:

When a person enrolls in e-commerce, he or she must provide Personally Identifiable Information (PII), such as their name, address, email address, telephone number, and credit/debit card numbers. If networks fail to ensure confidentiality and safety of customers information, the customers could suffer severe consequences. Criminals seeking to steal consumer financial and identity data from e-commerce web sites represent one of the top motivations for web hacking, according to an analysis from Trustwave, an Internet security firm.

Do you use online banking?

- ○ Yes
- ○ No

On a scale of 1 to 5, how convenient do you think online banking is for you

	1	2	3	4	5	
Not convenient at all	○	○	○	○	○	Extremely convenient

How often do you check your financial activity online

- ○ never
- ○ monthly
- ○ weekly
- ○ daily
- ○ Other: _____

Do you access your account from mobile devices (laptop, smartphone, Ipod, etc.)

- ○ Yes
- ○ No

Are you aware of the risks that come with Online Banking?

- ○ Yes
- ○ No

Please READ the following short paragraph that describes the most recent risks Online Banking has been related to:

When a person is enrolled in online banking, he or she may encounter phishing attacks or scams. Phishing is the process during which criminals send customers fake emails that are created to resemble the legitimate counterpart used by the bank, solely in an attempt to obtain a user's sensitive information. Malware is computer software that interferes with normal computer functions or sends personal data about the user to unauthorized parties over the Internet. Customers accessing their account from a computer infected with malware, could easily have their online account and thus financials compromised. Additionally, using the same password for multiple accounts online (refered to as password sloth) is another way through which online banking accounts are compromised. If criminals hack a users account in another website (i.e Facebook), and the user uses the same password to access his online banking account, the consequences could be severe.

Having read the risks mentioned above about social networking, e-commerce and online banking, do you think these services compromise your privacy?
Please answer for each.

	Yes	No
Social Networking	○	○
E-commerce	○	○
Online Banking	○	○

Do you think that being aware of the risks related to these services will change your attitude towards Internet privacy and your behavior online?

○ Yes

○ No

If answered "No" above, please briefly explain the reasons:

Would you reconsider the use of any of the services previously mentioned?
Please answer for each.

	Yes	No	Maybe
Social networking	○	○	○
E-commerce	○	○	○
Online banking	○	○	○

APPENDIX B

Okay, so first of all, thank you for volunteering to do this interview with us.
I'm just going to ask you a few questions, and you don't have to answer all of them.
If you feel uncomfortable answering a question, just let me know and we'll move on.
All your responses will be kept anonymous, and do you mind if we record this interview?
…Do you have any questions before we get started?

1. Have you taken or looked at the survey that was distributed online?

2. How long do you use the Internet for non-work and non-academic reasons each day?

3. Please rate your knowledge about internet privacy on a scale of one to five (one being no knowledge at all, five being extremely knowledgeable)

4. What factors do you think make an online service most desirable?
   ****After response:** "What about…popularity, visible confirmation of site security, site appearance, price of item or service?"

5. Here are some statements about the internet
   ****hand cards:** "What is your opinion on…?"

   Card 1: The providers of on-line services should be able to track the places users go on the Internet in order to send these users targeted marketing offers.

   Card 2: Consumers have lost all control over how personal information is collected and used by companies.

   Card 3: Most businesses handle the personal information they collect about consumers in a proper and confidential way.

   Card 4: Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

6. Do you find computer protective software to be beneficial?
   ****If yes**, what type(s) do you find useful?

7. What is your personal definition of Internet privacy?

8. Here is a definition of what a convenience is; please read it and let me know when you are done

   ****hand card**

   > **Card:** A convenience is defined as an online tool that allows users to complete a task with little effort. For example, e-mail may be considered a convenience because it allows users to communicate with others through the Internet in a faster method compared to the mailing of letters.

9. What is more important to you, convenience or privacy?
   Why?

10. Do you have an account on a social networking site?

    ****If yes:**

    - What sites do you use?
    - Why did you pick that/those sites?
    - Do you ever think about your privacy being at risk when on a social networking site?

11. How open are you online?
    What made you comfortable being at that level of openness?
    ****Reword if they express one extreme or the other**

12. Here is a definition of what a risk is; please read it and let me know when you are done

    ****hand card**

    > **Card:** A risk is defined as the possibility that an action or activity online will lead to an undesirable outcome. For example, if the action of a picture being posted online of someone that was of an unprofessional nature (such as nudity or intoxication due to the consumption of alcohol) was later seen by a potential employer. It could lead the undesirable outcome of the person losing a job.

13. What risks do you believe come with the use of social networks today?

14. Do you think the risks of social networking are great enough to compromise your (anyone's') privacy?

15. ****If yes to risks for social networking:** "What makes social networking still desirable to you, even though you know about the risks?"

16. Do you do any of your shopping online?

    ****If yes:**

    - What attracted you to online shopping?
    - What risks do you think come with online shopping today?

17. ****If yes to risks for online shopping:** "What makes shopping online still desirable to you, even though you know about the risks?"

18. Do you do any of your banking online?
    ****If yes:**
    - Are you aware of risks that come with using online banking?
    - Do you use mobile devices to check your bank information even though they make it easier for others to get a hold of your information?

19. ****If yes to risks for online banking:** "What makes shopping online still desirable to you, even though you know about the risks?"

Okay, that's all the questions I had for you.
Thank you for your time and for helping us with our IQP project.
Enjoy the rest of your day/night.

SOURCES CONSULTED

American Management Association (AMA), ePolicy Institute. (2005). *2005 Electronic Monitoring & Surveillance Survey.* Flynn, Nancy. Retrieved October 9, 2011, from http://www.epolicyinstitute.com/survey2005Summary.pdf

Anti-Phishing Working Group (APWG). (2010). *Phishing Activity Trends Report 2nd Half 2010.* Manning, Ronnie. Retrieved October 13, 2011, from http://www.antiphishing.org/reports/apwg_report_h2_2010.pdf

Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social engineering: Assessing vulnerabilities in practice. *Information Management & Computer Security, 17*(1), 53-63.

Benjamin, T., Juels, A., & O'Hare, T. (2009). Vulnerabilities in first-generation RFID-enabled credit cards. *Economic Perspectives, 33*(1), 50-51.

Chung, W., & Paynter, J. (2004). Privacy Issues on the Internet. *IEEE, 35*(1), 7-10.

Earp, J., Anton, A., Aiman-Smith, L., & Stufflebeam, W. (2005). Examining Internet Privacy Policies Within the Context of User Privacy Values. *IEEE, 52*(2), 227-236.

Electronic Privacy Information Center. (2005). *Privacy Self Regulation: A Decade of Disappointment.* Hoofnagle, Chris. Retrieved September 9, 2011, from http://epic.org/reports/decadedisappoint.pdf

Electronic Privacy Information Center (EPIC), Federal Trade Commission (FTC). (2012). *Civil Action.* U.S., Washington DC.

Federal Trade Commission (FTC). (2001). *The Gramm-Leach-Bliley Act, Privacy of Consumer Financial Information* (Public Law 106-102). U.S.

Federal Trade Commission (FTC). (2011). *Google Inc* (File No. 102 3136). U.S.

Gadzheva, M. (2007). Privacy in the Age of Transparency The New Vulnerability of the Individual . *Social Science Computer Review, 26*(1), 60-74.

Grobauer, B. (2011). Understanding Cloud Computing Vulnerabilities. *IEEE, 9*(2), 50-57.

Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies, 63*(1-2), 203-227.

O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. *Social Science Computer Review, 19*(1), 17-31.

Smith, Marcia S. (2005). Proceedings from CRS Report RL30784: *Internet Privacy: An Analysis of Technology and Policy Issues.* 109th Congress.

Smith, Marcia S. (2006). Proceedings from CRS Report RL31408: *Internet Privacy: Overview and Legislation.* 109th Congress.

Wang, H., Lee, M., & Wang, C. (2004). Consumer Privacy Concerns About Internet Marketing. *Communications of the ACM, 41*(3), 63-70.

Welborn, Angie A. (2003). Proceedings from CRS Report RL31919, *Remedies Available to Victims of IdentityTheft.* American Law Division.

White House. (2012). *Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights.* Office of the Press Secretary. Retrieved February 28, 2012, from http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

Zhang, Y., Chen, J., & Wen, K. (2008). Characteristics of Internet Users and Their Privacy. *Journal of Internet Commerce, 10*(3), 163-226.