KJR
Project Number: 52-KJR-1439

The Privacy Aptitude Test

A Novel Tool for Studying Factors that Affect User Internet Privacy Behavior

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

Benjamin E. Grossman-Ponemon

_____

Date: May 3, 2011

Approved:
Professor Kent J. Rissmiller, Major Advisor

_____

Abstract

The Internet has become ingrained in daily life. As the World Wide Web expands, offering new tools and services which allow users to connect in ways never before seen, the issue of Internet privacy becomes more important than ever.

The purpose of this study is to detail the construction and implementation of the Privacy Aptitude Test, a two-part exam which investigates users' knowledge of Internet privacy issues and their behavior online. Using the PAT and a brief personality test, I found that there was a positive relationship between users' knowledge of privacy issues and their behavior, and that certain personality types are associated different behaviors online.

Acknowledgements

As with any large undertaking, I would like to thank the following people for all their invaluable assistance on this project. I would like to thank Professor Rissmiller for all his guidance over the past three terms. (Time sure does fly when one's having fun!) I would also like to thank Professor Skorinko for allowing me to use the Psych Pool for my research. Finally, I want to thank Professor Smith for allowing me to use the Economics Laboratory, as well as for giving and teaching me the program z-Tree.

On the non-academic side, I would like to thank my father for all his privacy insight. Now, when someone asks me what my father does for a living, I have a much better idea on how to answer them! I want to finally take the time to acknowledge both my parents for all the hours spent listening to me rant about my ideas for this project, and for providing tuition so that I may attend WPI in the first place!

Table of Contents

Table of Figures

List of Tables

1. Introduction

Privacy is one of the most fundamental rights in the United States. In the Constitution of the United States, the right to privacy appears in the form of the Fourth Amendment. It states:

"The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (taken from Bill of Rights Transcript)

While this Amendment generally applies to unwarranted searching or invasion of one's home, it presents an expectation that all U.S. citizens are entitled to privacy.

As the Internet has become an integral part of people's lives, so too has the concept of Internet privacy. For the purposes of this paper, Internet privacy shall be defined as control over one's personal information on the Internet, including to whom or where one discloses the information. Internet privacy also refers to the expectation that an individual's personal information, even if disclosed on the Internet, is maintained or safeguarded in such a manner as desired by the individual.

Internet privacy sounds like a reasonable expectation. However, there are many instances that could be viewed as invasions of Internet privacy. For example, there are corporations which exist solely to monitor user behavior for advertisement or marketing purposes. Government may track what websites a user visits, which may be considered to be an "unwarranted search," and search engines remember what terms users input for up to 9 months.

The purpose of this paper is to better understand the factors that affect user privacy behavior. This includes how knowledgeable users are about Internet privacy issues and solutions, and whether or not personality has an effect on behavior.

Chapter 2 offers background on issues concerning Internet privacy, including some of those mentioned above, as well as user attitudes, government policies, and some solutions. With the background in place, the primary research questions are posed, and relevant literature is presented and analyzed.

Chapter 3 details the method of testing, including the makeup of the privacy aptitude test, as well as other testing instruments, and the procedure to be used when testing.

Chapter 4 details the data obtained in conducting the survey, and analyzes the results.

Finally, Chapter 5 offers concluding thoughts on the issue of Internet privacy, and what was found from testing. Remarks about the efficacy of the testing instruments and procedure, as well as goals for future research are given.

2. Background and Literature Review

2.1 Privacy Issues Facing Internet Users

The world of Internet privacy is diverse and ever-changing. To better understand some of the more important privacy issues facing Internet users, this section will provide information on certain issues, how users respond to these issues, and what the government and users do and can do about the issues. The goal of this section is to provide a clear background for the research at hand.

Behavioral Advertising

The Internet provides users with a myriad of services and options, most of which are free of charge (besides the cost of accessing the Internet). Like television channels, in order to gain revenue, website operators allow advertisers to place advertisements on their webpages. The hope is that the user may click on these advertisements and purchase some sort of product or service (A Primer on Behavioral Advertising).

There are two commonly used methods when advertising online: contextual advertising and behavioral advertising. Contextual advertising, often used on search engines such as Google, is accomplished by displaying ads that match the content of the web page. For example, a user visiting a dieting website may see advertisements for diet supplements or weight loss programs (ibid).

Behavioral advertising, on the other hand, bases the content of the advertisement on the user's previous browsing history. For example, a user who visits several dieting websites may see ads for diet supplements on his/her favorite news website. The advertisements have no relation to the content of the web page, but are based on where

the user has been beforehand. Advertisers, as well as websites, track the online behavior of a user using a cookie, a piece of data that records where a user has been or what settings a user has on a site (ibid).

This form of advertising poses several risks to user privacy. First, large quantities of user browsing data are collected, most often without the user's knowledge. This data may be sold to other companies or used in ways that are not consistent with the stated rationale for collecting the information (ibid).

While the advertisers do not collect personally identifiable information (PII), such as name or address, the depth of collected data may be great enough to identify a specific Internet user. For example, Acquisti and Gross from Carnegie Mellon University were able to predict an individual's Social Security number 8.5% of the time for birth dates between 1989 and 2003 by using known, often public, information (such as date of birth and location of birth), and by developing an algorithm based on known Social Security numbers. This study shows that even non-personally identifiable information, or fairly common public information, when combined, can often identify a user (Re-identification; Acquisti & Gross, 2009).

To make matters worse, behavioral advertising is an opt-out service: the user is by default subjected to the practice and must find a means to get out of being tracked. If these opt-out mechanisms even exist, they are often hidden on the website or are difficult to use properly (A Primer on Behavioral Advertising).

E-Commerce

Behavioral advertising techniques are also often applied to another common Internet service: e-commerce. E-commerce is the act of buying and selling goods on the Internet. This form of commerce has become incredibly popular as it allows customers to purchase goods from the comfort of home (Online Shopping Tips: E-Commerce and You).

However, just as with physical stores, there are risks to privacy associated with online shopping sites. To make a purchase, the merchant has to verify the consumer's identity and method of payment. This is often accomplished via the creation of an account, where the user inputs personal as well as payment data, including credit card numbers and expiration dates.

Giving information to an online party creates risks. First, if the website is not secure, or does not encrypt the information, there is the possibility of hackers obtaining user purchase information. Second, the website itself may sell the information of its users for profit (though this is not limited to e-commerce). Third, when creating accounts on websites, the user is often prompted with required fields, such as name, credit card number, or address, but merchants often include spaces for additional information. The most nefarious of these is Social Security. Giving out Social Security numbers can lead to identity theft, where a third party pretends to be the customer by making purchases in the customer's name or on the customer's credit cards (ibid). According to a 2006 Federal Trade Commission report, 3.7% of survey participants were victims of identity theft in 2005. This means that approximately 8.3 million U.S. adults discovered they were victims (FTC 2006 Identity Theft Report).

While not as explicit, there also is the risk of non-personally identifiable information collected by merchants being used to identify users. For example, in 2006, Netflix, which anonymously tracks its users' movie preferences, including movie ratings and date of ratings, published data on 500,000 of its users' behavior over a six-year period. While the data was anonymous, save for a unique identification number used for Netflix's tracking purposes, researchers, with 8 movie ratings and dates with up to a 14-day error, were able to uniquely identify 99% of user records (Re-identification; Narayanan & Shmatikov, 2008).

As with behavioral advertising, online stores often make use of behavioral marketing, where products are shown to customers based on previous purchases. For example, when viewing a product on Amazon.com, one may see related items, chosen to attract the customer. Like behavioral advertising, the stores make use of cookies to track user behavior. However, while it is possible to block these cookies, it may prevent the customer from making purchases (as online "shopping carts" are based on cookies) (Online Shopping Tips: E-Commerce and You).

Social Networking

Besides behavioral advertising and e-commerce, users face great risks to privacy when using social networking sites (SNS), such as Facebook, Myspace, or Twitter. With 500 million users on Facebook alone, these sites provide a great platform for connecting with friends and family; however, they introduce a whole slew of problems.

One of the most common problems, and one most often encountered by recent college graduates, is that users post incredibly compromising pictures of themselves or

their friends on SNS for all to see. Depending on the privacy settings of the individual user, such as who may or may not see the pictures, most anyone can view these images or links or other postings. Recently, employers have begun checking SNS in addition to traditional background checks. This can mean that the difference between getting hired or not may depend on what happened that one time at that party, or even worse, what one states his/her political views to be.

Even hired employees face being fired due to SNS. For example, Dawnmarie Souza was fired after criticizing her boss on Facebook. In response to her firing, the National Labor Relations Board filed a lawsuit against the company (Plocienniczak, 2010).

It is not only the workplace where too much on the Internet becomes an issue. In 2006, Stacy Snyder, a teacher-in-training, was denied her degree in teaching days before graduation because she had posted a photo of herself drinking at a party on her Myspace page. While her behavior was legal (she was over age, and all events were after hours), the university at which she was enrolled felt her behavior was "unprofessional," especially in front of her underage students. She filed a suit against the university, claiming violation of her First Amendment rights. However, in 2008, a federal district judge turned down the case (Rosen, 2010).

As one can see, showing too much can be an issue. However, there are times when what one shows is out of his/her control. When Facebook introduced the News Feed feature, where user posts are shown to all friends, many were unhappy, and even petitioned Facebook to remove the feature. To date, this feature has not been removed (Facebook Privacy).

Another area of social networking sites where user privacy is an issue is the sharing of information to third parties via Internet games. Online games, such as Farmville or Mafia Wars (two popular games on Facebook), require access to user information before playing. This information includes, but is not limited to, the user's profile picture, date of birth, networks, and list of friends (ibid).

How Users Respond to Privacy Issues

Users' Internet behavior often contradicts their stated preferences or concerns for privacy. According to Van Dyke, while users claim that privacy is important, they often perform risky behavior. Van Dyke says, "According to one study, users rejected fewer than 1% of cookies in over a billion page views." He further explains, "It is possible that many who believe they are making informed, rational decisions are, in fact, making irrational decisions based on an unrecognized ignorance of the technologies, laws, and data flows related to online information gathering" (Van Dyke, 2009).

Several studies by the Ponemon Institute illustrate the contradiction between users' concerns for privacy and their behavior or intention to use privacy protection strategies. In a 2010 survey on the newly implemented full body scanners in airports, the Ponemon Institute found that 79% of respondents viewed the protection of privacy rights as "Very Important" or "Important." Furthermore, 69% of respondents indicated that they were "Very Concerned" or "Concerned" about full body scans as part of airport security procedures, while 79% showed concern at pat-down searches. However, when asked if respondents would opt for an alternative procedure which caused delays of 1, 5, and 10 minutes, respondents indicated they would choose the procedure 65%, 21%, and 9% of

the time, respectively. These findings show that respondents favor convenience (in this case, fewer delays) even though they indicate concerns for the practices in use (Ponemon 2010).

In another 2010 Ponemon survey on user concerns and behavior when using social media sites (such as SNS), while 74% of the general sample and 77% of the identity theft sample viewed protection of their privacy as "Very Important" or "Important," there was virtually no difference in behavior between the two groups. Victims of identity theft showed nearly the same behavior on SNS as those who weren't victims. These findings are completely contrary to the idea that identity theft victims are more protective of their personal information (Ponemon, 2010).

Besides an ignorance of laws and technology as indicated in Van Dyke's literature, and an element of convenience in the Ponemon Institute surveys, the disconnect between concerns and practices in Internet privacy may arise for the same reason that it does for other risky behavior, such as gambling or text messaging or using cell phones while driving: there is an interplay between the risks and benefits offered by the behavior.

In the case of using a cell phone (either for calling or text messaging), there are clear risks to personal safety, mostly in the form of distraction from the road. However, people persist in making phone calls or sending text messages. Perhaps to these individuals, the risk to personal safety is outweighed by the instant gratification or convenience of making a phone call or sending a text message from anywhere at anytime.

Government Response to Privacy Issues

Because of the technology explosion in recent years, especially as it relates to the world of the Internet, it is difficult to apply established case law to completely new situations not envisioned by the writers of those laws. Over the years, the United States government has implemented several laws to protect users on the Internet. One of the earliest is the Privacy Act of 1974, which has several provisions for the compiling of user data on computers. This includes how much data can be collected and who can use the data (The Privacy Act of 1974).

In 1986, the United States introduced the Electronic Communications Privacy Act (ECPA), which was designed to regulate government access to electronic communications. Under the ECPA, the government could legally subpoena Internet Service Providers (ISP) to get IP addresses, or other information about individual users. Other notable laws protecting user privacy from the government include the Protect America Act (PAA), which was introduced in 2007 in response to the Bush wiretapping scandal. However, these laws primarily deal with government surveillance and collection of information by the government (Basset & Buckley, 2010).

Laws protecting users from tracking or other forms of data collection by businesses are much more lacking. This is due to the fact that Internet access is (often) run by a private entity, the ISP. Users are paying for access to the Internet, and for the services provided. Thus, the Internet currently runs on a model of self-regulation (Van Dyke, 2009).

However, recently policy makers have been constructing measures to protect Internet users. According to a New York Times article by Wyatt and Vega, the Federal

Trade Commission is advocating a "do not track" mechanism, in the same way a "do not call" list protects people from telephone solicitors. Like the "do not call" list, Internet users could sign up for a "do not track" feature, which would prevent advertisers from tracking user behavior. However, this would not prevent "basic targeted advertising" where ads are generated in response to search terms (as seen on Google). Also, such a list or feature would deal a blow to online advertisers, who generate much of their income by collecting personal data. Regardless, the proposition of such a measure shows that the self-regulation model currently in use is not as effective as it may seem (Wyatt & Vega 2010).

What Users Can Do to Protect Privacy

As the Internet operates on a system of self-regulation, it is up to the user to protect his/her privacy to the fullest extent possible. There are several tools available through Internet browsers that can protect privacy, such as private browsing options and ad-blockers, and there are services, which may be costly, to fix up a user's Internet "presence," the most common of which are reputation defenders or cleaners.

Internet browsers either come with, or have available, add-ons or other software that can help a user maintain privacy on the Internet. The first is a private browser. A common feature in most browsers, such as Firefox or Internet Explorer, private browsing is a feature that prevents the browser from "remembering" browsing history. Private browsers often also do not store cookies, entered passwords or search bar entries. However, private browsers do not make users anonymous on the Internet. The troubleshooting page for Firefox's private browsing clearly states: "Private Browsing

prevents information from being recorded on your computer. It does not make you anonymous on the Internet" (Private Browsing - Firefox Help).

Some Internet browsers, such as Firefox, offer add-ons that prevent data collection or advertisments, etc. One example is BetterPrivacy, which deletes persistent cookies, such as Flash cookies (compared to standard HTML cookies). These cookies are difficult to delete or are hidden on the computer (BetterPrivacy - Add-ons for Firefox). Another add-on is NoScript, which blocks all scripts except those allowed by the user. This helps prevent users from encountering malicious scripts or other unwanted items on a webpage (NoScript - Add-ons for Firefox). Finally, another useful add-on is AdBlock Plus, which, as its name implies, blocks advertisements or other unwanted items (AdBlock Plus - Add-ons for Firefox). These are just a few of the available software that provide users with some capacity to control the cookies on their computers and the advertisements encountered while on the Internet.

For cases of posting "too much" on the Internet, such as those mentioned above, a new business sector has been created: reputation defenders. While advertisers collect information to sell products to users, reputation defenders monitor online behavior, contacting websites to take down undesired material, and use search engine techniques to change the "relevancy" of undesirable search results. The end goal is to eliminate, or hide well, unwanted items on the Internet, such as compromising photographs or videos. This service is especially relevant to job hunters, as employers make use of search engines or SNS to perform background checks (Rosen, 2010).

Finally, one of most effective techniques is to simply be careful on the Internet. First, users can delete cookies on a regular basis. Another good practice is to read the

privacy policy of websites. This allows users to better understand how the websites collect data. For example, search engines will remember IP addresses and searches for various amounts of time, before either deleting or anonymizing the IP address. While Yahoo will remember for 90 days, Google keeps data for 9 months (Online Privacy: Using the Internet Safely).

On social networking sites, users can protect themselves by restricting access to their profiles (such as who or what others can see). Third-party applications provide a means of accessing personal information, so care should be exercised when allowing them. Finally, in the case of job hunting or employment, or other areas where reputation may be important, users should take caution as to what images or videos exist of themselves on social networking sites, as well as what they post (Social Networking Privacy: How to be Safe, Secure and Social). In an article on social networking etiquette, Tyson B. Snow, an employment attorney, is quoted, "Imagine if the comment you posted or tweeted will appear in the local newspaper the next day" (Chen, 2010).

For those who want more information, the Electronic Privacy Information Center (epic.org), Privacy Rights Clearinghouse (privacyrights.org), and the Center for Democracy & Technology (cdt.org) offer primers and fact sheets on numerous privacy issues, and provide users with steps to protect their privacy.

The Need for a Privacy Aptitude Test

With the presence of many online privacy issues, the lack of understanding on the part of users, the inability of government to regulate, and the sheer inability of users to stop information tracking, there seems to exist a need for self-evaluation of the risk of a

user's online behavior. To this end, I propose the creation of a privacy aptitude test, a proficiency exam that gauges a user's understanding of privacy and his/her capability to maintain privacy during online excursions. The outcome of the test, the end result the user receives, is a privacy score, akin to a credit score, or even an IQ, a score that ranks the user on a scale from a low privacy aptitude to a high privacy aptitude. This score allows users to see how they perform, and hopefully increase privacy awareness and foster a desire for better scores.

As stated, I believe privacy aptitude is composed of two parts: knowledge and behavior. How much a person knows about privacy would indicate his/her understanding of privacy issues, while their behavior indicates how much they actually do to maintain their privacy.

The proposal of a privacy aptitude test opens the doors to a multitude of research questions and possibilities. However, the most important question raised by a privacy aptitude test, especially if the end result is quantified, would be what factors affect privacy aptitude, the combination of knowledge and behavior? Particularly, what factors affect user Internet privacy behavior, such as users' privacy settings and how much information users give online?

As I believe privacy aptitude is a composite of both knowledge and behavior, it follows that the primary research question of this paper is whether there is a relationship between knowledge of privacy issues and topics and a user's privacy behavior (i.e. would more knowledge mean more secure behavior, and vice versa). As the privacy aptitude test is composed of two parts, however, there are (roughly) four possible outcomes expected:

a combination of either having knowledge or not, and either exhibiting "good" privacy behavior or not. An array showing the possible outcomes is shown below:

	Behavior	
Knowledge	High Knowledge, Good Behavior	High Knowledge, Poor Behavior
	Low Knowledge, Good Behavior	Low Knowledge Poor Behavior

Table 1: Outcomes of a Privacy Aptitude Test

This first topic investigates if those who have more knowledge exhibit "better" behavior, and vice versa (i.e. the main diagonal elements of the above array).

However, as shown, there are the two off-diagonal outcomes: those who have knowledge of privacy issues but do not exhibit good behavior, and those without knowledge who exhibit good behavior. These outcomes raise the question: if a knowledge of privacy issues does not always affect user behavior, then what else would? Is there a reason why a user who knows about privacy issues would not necessarily have good behavior, etc? Does it have anything to do with personality? Thus, the second research question is raised: Does personality have an effect on user privacy behavior? For example, is an extrovert, even if he/she knows about privacy issues, more likely to exhibit poor behavior than an introvert or recluse?

Finally, while not a formal research question, I believe that, as the proposal of the privacy aptitude test is in itself an ambitious claim, it is necessary to debrief the test takers to verify the proposal. Does the test do as it should: are the scores of the privacy aptitude test accurate? Do respondents react to their scores? Do they see the scores as a means of self-improvement? Are the results of a privacy aptitude test important, valuable, and useful to the respondents? Further questions under this topic include whether or not

users would desire to change their behavior in response to their scores (as in, is the test a motivator for change)? The validation of the test is an important and fitting conclusion to this paper.

Following is a literature review of materials that are relevant to the three issues presented above. The research that exists on these topics will be investigated and discussed in relation to the proposed research topics.

2.2 Knowledge and Privacy Behavior

Statement of the Research Question

The privacy aptitude test provides a metric to grade a user's proficiency in Internet privacy. To test a user's aptitude, a two-part examination is performed: the first tests a user's knowledge of privacy issues and the second examined a user's privacy behavior. It follows from such a test format that the first research question asks if there is a relationship between a user's knowledge of privacy issues and his/her privacy behavior. Stated formally:

> Is there a relationship between an individual's requisite knowledge of Internet privacy and the level of risk of his/her behavior on the Internet? Specifically, will a higher level of privacy knowledge result in more cautious behavior? Conversely, will a low score result in reckless behavior? Examples of cautious behavior include the use of private browsing, ad blockers, and the deletion of cookies on a regular basis. Examples of reckless (or risky) behavior include posting videos or photos of oneself to social networking sites, or the giving of personal information to third parties.

It is necessary to define several terms in the problem statement. Risky or reckless (the two will be used interchangeably) behavior refers to behavior that exposes user information, either voluntarily or involuntarily, to unwanted parties. This includes giving more information than necessary when creating an account for a website, or sharing photos or a profile on a social networking site without limiting access to said photos or profile. In contrast, cautious behavior is defined in this paper to be that which takes care to protect user information. As the opposite of reckless behavior, cautious behavior includes limiting access to profiles or pages on a social networking site, or regularly blocking or deleting tracking cookies.

Literature Review

Research on the relationship between user knowledge of privacy and privacy concerns and behavior is limited. Studies have been performed testing users' knowledge of privacy, their awareness of privacy protection, and their use of protection strategies (Dommeyer & Gross, 2003), on users' knowledge of information security and their readiness to adopt security solutions (Wang, 2010), and on the effects of privacy education on the level of privacy concern (Van Dyke, 2009).

Dommeyer and Gross' study, published in 2003, tested users' knowledge of privacy in relation to telephone, mail, and Internet purchases, and their awareness and use of privacy protection strategies. (Please note that in 2003, Internet purchases made up a much smaller percentage of consumer activity.) There were four hypotheses tested: effect of gender, age, unlisted telephone status, and a person's desire to receive solicitations from direct marketers on awareness and usage of privacy protection strategies, Dommeyer and Gross made use of a two part test. The first part was a true-false test, where the respondents were given statements that tested knowledge of privacy law. The second part tested both awareness and use of privacy protection strategies. The respondent was given statements, such as "I do not purchase items by telephone," and was asked to respond either "Unaware of Strategy," "Aware, but Have Not Used," and "Have Used Strategy."

The first part was graded on a correct/incorrect scale, and users received a score out of the number correct. To grade user awareness on the second part, responses of "Aware, but Have Not Used" and "Have Used Strategy" were considered signs of awareness. The respondent was then given a score of how many strategies they were

either aware of or used. To measure use of strategies, only answers of "Have Used Strategy" were marked toward the scores.

Dommeyer and Gross found that respondent knowledge of issues was very poor, with a mean score of 2.95 out of 10. They concluded that a lack of knowledge was observed in previous studies, and attribute the low scores to ignorance of issues. Specifically, Internet privacy issues were much more in the public awareness, compared to issues arising from the use of telephone or mail.

The average score on the awareness tests, unlike knowledge test, was found to be much higher, with an average of 17.95 out of 26. However, the average scores of the usage test was lower at 7.90 out of 26 (as was expected, since responses in the "Aware, but Have Not Used" category would be deemed correct on the awareness test, but incorrect on the usage test).

The Dommeyer and Gross testing method is very interesting and has several advantages. First, the knowledge test presents situations and sees whether or not the responder knows if the situation is true or false. Compared to a multiple choice test, where there are several solutions, there are only two options. However, as there are more options for multiple choice, the chances of random guessing yielding correct answers is increased in a true-false test.

The second part is particularly interesting as it tests two areas at once: awareness and usage of privacy protection strategies. As this part has no "incorrect" answers, responders are free to answer as they please.

The Dommeyer and Gross study, however, is relatively "old." Published in 2003, its focus was more on users' use of privacy protection strategies and their knowledge.

This study focused more on telephone solicitation, mail, and personal encounters, rather than online behavior. Furthermore, social networking sites were in their infancy: Myspace was just founded, and Facebook was not developed until 2004. Thus, issues concerning the use of social networking sites were not apparent at the time. If such a testing method were to be used, it would have to be modified to focus on Internet privacy, and include modern privacy issues such as social networking.

Ping An Wang's study, published in 2010, is much more current, but the focus is on technology adoption behavior (what factors affect people's desire to adopt certain technologies).

To test users' likelihood to adopt technologies, he used Likert scale questions, where 1 corresponded to "Strongly Agree" and 7 to "Strongly Disagree." Questions were based around the areas of research of his study: knowledge of security solutions, experience with security solutions, attitudes toward security solutions, and intention to use security solutions.

Wang found that the highest correlation occurred between attitude and intention, with a Pearson correlation coefficient of 0.783, while the correlation between knowledge and intention was 0.701. This data means that there was a fairly strong correlation between users who had a positive attitude toward security solutions and their intention to use said solutions. However, he found that there was a correlation between knowledge of security issues and intention to use security solutions. This means that the more people know about security issues, the more likely they are to use solutions. Perhaps there is a similar association for overall privacy knowledge and behavior.

Wang's study, unlike Dommeyer and Gross's, is more focused on user adoption of security solutions. Furthermore, his method is not clearly explained, which makes understanding what he did very difficult.

Van Dyke, on the other hand, took a completely different approach to knowledge and privacy practice. In his 2009 study, Van Dyke tested the effects of privacy education on privacy behavior.

Van Dyke's study consisted of asking users their level of privacy concern with a two level Likert scale, and then a series of two yes/no questions on the respondent's e-commerce preferences. Upon completion of the study, the users were then presented with a demonstration of the capacity of information collectors (a brief list of items that advertisers could collect). Respondents then retook the test with the information presented in mind.

Van Dyke found that concerns for privacy increased after the demonstration, from a mean of 3.112 to a mean of 3.419 (out of what value, the author does not make clear).

Van Dyke's testing method is interesting, but does not seem in depth enough for a privacy test. Furthermore, he does not test the knowledge of privacy of the respondent, but rather sees if a brief education piece has any effect on users' preferences. Regardless, his study does show that knowledge has an effect on preferences and privacy concerns.

Conclusions

Research on the relationship between knowledge of privacy and privacy practice is very limited, if not non-existent. While Dommeyer and Gross's study tests knowledge of privacy law and issues, as well as the use of privacy solutions, it does not compare the

two. There was no indication of whether those with knowledge of privacy used privacy protection solutions to any greater or lesser extent. Wang's study found that there was a correlation between a user's knowledge of security and his/her intention to adopt security solutions. Finally, Van Dyke's study found that educating users on privacy issues will increase their concerns.

However, it seems that research on the relationship between privacy knowledge and privacy behavior is unbroken ground. This paper attempts to fill in this missing ground.

2.3 Personality and Privacy Behavior

Statement of the Research Question

Knowledge of Internet privacy is not the only influence on privacy behavior. In addition to knowledge, it is predicted that personality would affect how a user conducts himself/herself on the Internet. Thus, the second research question seeks to know whether or not personality has an influence on privacy behavior or privacy scores. Stated formally:

> In addition to knowledge of Internet privacy, is there a relationship between an individual's personality and his/her privacy behavior? For example, is an extrovert more likely to have risky behavior than an introvert? Also, is there a relationship between an individual's personality and his/her privacy scores? For example, would a nervous individual be more likely to exhibit good behavior regardless of his/her knowledge?

Before seeking out what research exists on the relationship between personality and privacy practice, it is necessary to first understand personality psychometrics. There exist several metrics. One of the most famous is the Myers-Briggs Type Indicator (MBTI), a test that tests four areas: introversion and extroversion, sensing and intuiting, thinking and feeling, and judging and perceiving. This yields sixteen possible outcomes. (Lilienfeld, Lynn, Namy & Woolf, p570)

Another personality psychometric is the Big Five (or Five Factor) Model, which analyzes personality using five categories or criteria. These categories arise from the idea that the most important ideas or items are those which people frequently talk about. These five items are Openness to Experience (or Openness), Conscientiousness, Extraversion, Agreeableness, and Neuroticism. Openness (or Intellect) refers to those who are "intellectually curious and unconventional" (Lilienfeld et al., p562). Conscientiousness refers to being "careful or responsible" (Lilienfeld et al., p562).

Extraversion refers to those who are social. Agreeableness refers to those who are "easy to get along with" (Lilienfeld et al., p562). Finally, Neuroticism refers to those who are "tense and moody" (Lilienfeld et al., p562).

Unlike the Myers-Briggs Type Indicator that classifies people into categories based on four criteria, the Big Five Model sees which personality types are dominant. Due to the more simplistic nature of the Big Five Model, it is more often used in studies.

Literature Review

There is much research in the relationship between personality and Internet privacy. Bansal, Zahedi, and Gefen investigated the impact of personal disposition on disclosure of health information. In their 2010 study, they analyzed various factors that affect users' desire to disclose health information online. One component of the study focused on personality and the perceived sensitivity of health information. To study personality, Bansal et al. used the Big Five model. They anticipated that there was a negative association between Extraversion and Openness and the perceived health information sensitivity. Conscientiousness, Agreeableness and Neuroticism, they hypothesized, had a positive association with perceived health information sensitivity.

To conduct their test, Bansal, Zahedi, and Gefen used a rating scale test, where respondents are given statements and have to indicate their agreement on a scale from 0 (strongly disagree) to 10 (strongly agree). A similar test was given for health information sensitivity. Again, respondents answered between 0 (not sensitive at all) and 10 (very sensitive).

Bansal, Zahedi, and Gefen found that people with high Openness had lower perceived sensitivity of health information, while those with high Neuroticism and Agreeableness had higher perceived sensitivy, in accordance with their hypotheses. However, they did not find a significant relationship between Extraversion and Conscientious and perceived sensitivity. In response to finding an insignificant relationship between Extraversion and perceived sensitivity, Bansal et al. concluded that there may be a social stigma against sharing information online, or that extraverts may exhibit different behavior online.

In 2008, Korzaan and Boswell did a study on personality traits and concerns for information privacy (CFIP). Like Bansal et al., Korzaan and Boswell used the Big Five Model for their personality testing. They hypothesized that Extraversion, Agreeableness, and Conscientiousness would have a positive influence on CFIP, while Conscientiousness, Neuroticism, and Openness would have a positive influence on computer anxiety.

Like Bansal et al., Korzaan and Boswell used a Likert scale test (the number of levels is not specified) for personality testing, which allowed them to score, based on level of agreement with statements, individuals' personalities. They also used a Likert scale to test concerns for information privacy and computer anxiety.

Korzaan and Boswell found that the only supported hypotheses (of personality on CFIP and computer anxiety) were that there was a positive relationship between Agreeableness and CFID, a positive relationship between Neuroticism and computer anxiety, and a positive relationship between Openness and computer anxiety. The hypothesis that there was a positive relationship between Extraversion and CFID was not

supported, and neither were the hypotheses involving Conscientiousness. These results coincide with those of Bansal et al., in that no conclusions could be drawn about Extraversion and Conscientiousness. However, as there are differences between CFID or computer anxiety and perceived health information sensitivity, the two are not completely comparable.

Another study on the relationship between privacy concerns and personality was conducted by Friberg in 2007. Like Korzaan and Boswell, Friberg utilized the Big Five Model when studying personality. He hypothesized that personality would have an effect on privacy concerns and Internet privacy concerns (he makes the distinction between the two).

To test the personality of an individual, Friberg made use of the Ten-Item Personality Inventory (TIPI). The method of testing is to provide ten sets of two phrases or adjectives, and the respondents must state how much they feel the adjectives describe themselves, with an answer being one of seven levels of agreement, from "Disagree Strongly" and "Agree Strongly." The test is designed that six consecutive statements test for certain components of personality. In his case, for example, statements 1 to 6 tested Extraversion, 2 to 7 Agreeableness, etc. Instead of Neuroticism, he used Emotional Stability (in essence, the latter is the inverse of the former). To test levels of privacy concern, Friberg used a Likert scale test.

In testing privacy concerns and personality, Friberg found that there was a negative relationship between Emotional Stability and concerns for privacy. Likewise a similar relationship existed for Agreeableness and privacy concerns. Friberg also found that there was a positive relationship between Conscientiousness and privacy concerns. Finally, contrary to what was predicted, there was a positive relation between Openness and privacy concerns. Results for Internet privacy concerns and personality were similar.

Conclusions

In studying literature on personality and privacy behavior, researchers have found that an individual's personality has an effect on how he/she perceives privacy or his/her concerns for privacy. There are several methods for testing personality in a brief period of time. Most studies make use of the Big Five Model, versus the more in-depth Myers-Briggs Type Indicator. Also, most studies use some sort of Likert scale to test respondent's level of agreement with certain statements. However, the actual testing method differs. Bansal, Zahedi, and Gefen and Korzaan and Boswell provided a couple of statements for each personality element. Friberg, on the other hand, made use of the Ten-Item Personality Inventory, where the entire personality screening process was reduced to ten Likert scale statements.

Overall, I feel that the TIPI method employed by Friberg appears to be the simplest and easiest to use. As it is only composed of ten items, compared to several per personality type, the TIPI is more compact, meaning it is easier to complete.

Finally, the literature studied focuses primarily on how personality affects concerns for privacy. As mentioned earlier, there is often a disconnect between an

individual's concerns for privacy and his/her actual behavior. Thus, the Likert scale method of testing used for privacy concerns may not be useful for the purposes of this research. However, it is interesting to observe the effects of personality on privacy behavior, and how these effects compare to those of personality on privacy concerns (whether the influence of personality carries through from concerns to actual behavior).

2.4 Debriefing of the Privacy Aptitude Test

The final topic of this paper is the validation of my proposed privacy aptitude test. This validation determines if the results of the test match actual behavior. For example, in the case of the privacy aptitude test, it is necessary to make sure that a user who scores poorly truly exhibits risky behavior.

Furthermore, as the privacy aptitude test is envisioned to be a tool of self-evaluation, it is necessary that respondents react to their scores either in agreement with them, or showing surprise when different than anticipated. Do respondents find the results of the test (their scores) to be important, valuable, and useful?

If the privacy aptitude test is to be a tool of learning, then would respondents learn from the test? I believe that the privacy score, much like a credit score, can change depending on the actions of the user. As a user becomes more aware of privacy solutions or learns more about privacy issues, it is envisioned that privacy scores may improve. From this idea, the following question can be extrapolated: Will users who score poorly on the privacy aptitude test desire to improve (at least in the short term) their privacy scores?

Relevant Literature

As the idea of whether or not a test is successful is not a formal research question in the same vein as the previous two, it is difficult to find literature on this topic. However, certain studies did provide some insight.

Van Dyke's survey, described earlier, showed that a demonstration can cause a change in respondents' concerns for privacy. In addition to the concerns for privacy

questionnaire, Van Dyke also asked the respondents two "yes or no" questions regarding their preferences for websites. These included whether or not respondents wanted websites to remember them when they visit again, and if they wanted websites to recommend items based on their previous visits.

Van Dyke found that there was a shift in user responses from the pre-test to the post-test. For the first question, 24 of the 49 respondents, and 17 of 47 for the second question, who answered "yes" initially changed their responses to "no" following the demonstration. This means that a demonstration or display of the risks of Internet privacy can cause a change in users' behavior. Whether or not these people went on to permanently change their behavior is unanswered.

In terms of the effects of a learning tool on user's behavior, Wills and Zeljkovic constructed a website that, based on users' browsing history, attempted to predict demographic information, such as age and gender. Their website, whattheyknow.cs.wpi.edu, also provided followup research questions which asked about respondents' use of privacy protection strategies. While the study never tested the effectiveness of the website as an instructional tool or its role in behavior change, Wills and Zeljkovic did receive feedback indicating a favorable opinion of the website.

This research suggests that surveying tools may indeed affect user opinions and behavior. However, unlike Wills and Zeljkovic, I intend to survey changes in user attitudes and test for changes in behavior.

2.5 Concluding Remarks

I have presented some background of the issues surrounding Internet privacy, user reactions, and some suggested solutions. I have introduced and explained my three research goals, and have presented a discussion of pertinent research.

I have found that there is not much research on the relationship between knowledge and privacy behavior. This is a gap I believe needs to be filled.

The relationship between privacy behavior and personality has been studied to a greater extent. This research material included information on effective personality testing. However, the focus of the research was primarily on concerns for privacy and not actual behavior. The research presented in this paper is new and unique in its attempt to investigate and score privacy behavior.

Finally, such a privacy aptitude test needs to be verified. This includes making sure the test accurately reflects the behavior of the respondents, and that the test promotes self-evaluation and a desire to improve. Furthermore, I intend to examine whether users will desire to change their behavior in response to the test.

3. Methodology

In this section, I explain how my privacy aptitude test was constructed. I also describe the procedure by which the test was implemented. Finally, I will make clear how I intend to answer my research questions.

3.1 Privacy Aptitude Test

The following is a complete description of the design of the privacy aptitude test. Because this is a new idea, there is no model on which to base it. Thus, procedures to construct the test from the ground up are detailed below.

Purpose

The purpose of the PAT was to categorize and quantify both a person's privacy behavior and understanding of privacy. In short, I desired to create a privacy psychometric.

Method

The PAT was a two-part test: one part measured a person's knowledge or understanding of privacy issues. This component of the test asked the respondent a series of multiple choice questions concerning various privacy issues or concepts. To eliminate random guessing, the option of "Do not know" was given for each question. The following is an example of a multiple choice question:

1. Which of the following is not Personally Identifiable Information (PII)?
    a. Name
    b. Address
    c. Social Security

d. Date of Birth
e. Do not know

The correct answer is d. Date of Birth.

The second part of the test was a behavioral survey of the respondent. This section asked questions about how the user behaves online. Depending on how the answer compares to prudent privacy behavior, a score was be given. Examples of behavioral questions:

2. Do you use a social networking site (SNS)?
Yes
No

3. Do you use ad blocking tools?
Yes
No

4. How often do you delete cookies?
Often
Sometimes
Rarely
Never

Scoring

The score of a PAT, dubbed the Privacy Score(s), was given in a two-number format. The first represented the score on the knowledge test, the second on the behavioral test. These two scores were presented as an ordered pair.

The privacy score is similar to a credit score. Just as a lower credit score indicates that a person would not pay bills on time or reach a credit limit quickly, a privacy score indicates how likely a person is to share sensitive information over the Internet or allow advertisers or unwanted third parties to obtain information. Essentially, both are measures of the risk of an individual's privacy behavior.

The knowledge test was graded based on a right-wrong basis. Each correct answer

was awarded 1 point, while incorrect answers were given a -1. Answering "Do not know" also yielded a -1 score for the question. The final score was then normalized to a range of -1 to +1 (by dividing the raw score by the number of questions). In total, there were 16 graded questions, with a 17th as an extra (the complete set of questions is given in Appendix B).

The behavioral test is also normalized to the same -1/+1 scale as the knowledge test. However, scoring for the behavioral test was different. The responses to each question were graded based on a risky versus safe basis. The total possible points for any given question ranged from +1 to -1. This means that on a question with four responses, the safest response was given a +1, the next response a +0.33, next a -0.33, and the last response a -1. This ensures that a sense of neutrality is maintained. Some questions were graded with slightly more weight. For complete scoring rubric, please see Appendix A.

Outcomes

With the two part test, I expected two outcomes for each test: those who are knowledgeable of privacy or not, and those who have good privacy behavior or not. Thus, there are four possible outcomes, illustrated using the following table:

	Behavior	
Knowledge	High Knowledge, Low Risk Behavior	High Knowledge, High Risk Behavior
	Low Knowledge, Low Risk Behavior	Low Knowledge High Risk Behavior

Table 2: Privacy Aptitude Test Outcomes

This sort of table is similar to that used in the Myers-Briggs Type Indicator test. Using the above categories, the tester can make observations about people's privacy practices. The following are descriptions of the anticipated meaning of the outcomes.

People who are knowledgeable and have good practice are very privacy conscientious and care very much about their PII. They want to minimize their risk on the network. This is the preferred outcome.

People who are knowledgeable but have poor practice may know about the issues, but either do not care about maintaining good privacy practice or do not have access to privacy tools.

Those in the unknowledgeable and good practice category seem to perform well and may care about their privacy, but they do not have a good understanding of the issues. It may be in their benefit to read up or properly understand the issues.

Finally, those who are unknowledgeable and have poor practice are at high risk for privacy breaches. They do not maintain good standards, nor do they have any understanding of the issues. Perhaps if informed, they may change their practices, but at this point they are undesirable for information sensitive jobs.

For the actual test itself, to create more personalize results pages, I created nine outcomes. These correspond to knowledge and behavior scores between -1 and -0.33, -0.33 and 0.33, and 0.33 and 1.

3.2 Personality Test

To test a user's personality, I used the Big Five Model (Extraversion, Openness, Conscientiousness, Neuroticism, and Agreeableness). To quickly and easily identify the user's personality, the testing method of Friberg was used.

Friberg used the Ten-Item Personality Inventory (TIPI), where the respondent's personality is determined from ten questions. The respondent is given ten sets of

adjectives or phrases, and must state his/her level of agreement with how well the adjectives describe him/herself. Friberg's test is shown below:

Disagree Strongly	Disagree moderately	Disagree a little	Neither agree nor disagree	Agree a little	Agree moderately	Agree strongly
1	2	3	4	5	6	7

I see myself as:

1. _____ Extraverted, enthusiastic.
2. _____ Critical, quarrelsome.*
3. _____ Dependable, self-disciplined.
4. _____ Anxious, easily upset.*
5. _____ Open to new experiences, complex.
6. _____ Reserved, quiet.*
7. _____ Sympathetic, warm.
8. _____ Disorganised, careless.*
9. _____ Calm, emotionally stable.
10. _____ Conventional, uncreative.

*In the analysis, these items are reverse scored (R).

Figure 1: Ten-Item Personality Inventory (Friberg 2007)

Friberg details that questions 1 to 6 test Extraversion, 2 to 7 test Agreeableness, 3 to 8 test Conscientiousness, 4 to 9 test Emotional Stability (the opposite of Neuroticism), and 5 to 10 test Openness.

As such a test is very short, it seemed ideal for this research (as the privacy aptitude test may be long or time consuming).

3.3 Post-Questionnaire

To verify the functionality of the privacy aptitude test, as well as determine respondents' reactions to the test itself, a post-questionnaire was given.

Upon completion of the test, the respondents were presented with their privacy scores, and a brief description of the meaning (which depended on the score range in which they fell, as explained in the Scoring of the PAT).

The respondents were then prompted with a followup survey. Some examples of

questions similar to those asked in the followup (The complete post-questionnaire is given in Appendix C):

1. How does your knowledge score compare to your expectations?
    a. Higher than expected
    b. Lower than expected
    c. As expected

2. Does the accompanying descriptor of your score accurately reflect your privacy habits?
    a. Yes
    b. No

3. Are you satisfied with your privacy score?
    a. Yes
    b. No

4. Would you like to know how to improve your scores?
    a. Yes
    b. No

5. Do you feel the privacy aptitude test was informative?
    a. Yes
    b. No

The overall purpose of the followup was to see if the score accurately reflects the level of risk of a user's privacy behavior, as well as his/her overall knowledge of privacy. Also, the post-questionnaire sought to ask if the user was satisfied with his/her score and if he/she would like to learn more information about how to improve his/her scores (and, by extension, lessen his/her risk). The post-questionnaire sought to determine if the test was informative and useful to the respondent.

3.4 Testing Subjects and Location

The respondents for the test came from the "Psych Pool," undergraduate students enrolled in psychology or economics courses who are recruited to participate for credit.

The test was administered in SL223A, the Economics Laboratory (under

Professor Alexander Smith). The test was on computers, and the software z-Tree was used to construct and administer the test.

As the test was limited by the size of the laboratory, a maximum of 12 students at a time could take the test. Overall, seven sessions were held, with a total of 45 respondents participating.

3.5 Testing Procedure

The test began with the TIPI personality test. Upon completion of the personality test, the respondent was given the privacy aptitude test, knowledge questions first. Using the scoring mechanism, the respondent was then given his/her privacy scores, and the accompanying information and descriptions. Because of the limitations of the software, a knowledge-behavior graph handout had to be given to each respondent. Then, the user was presented with the post-questionnaire. Finally, some simple demographic information was collected (class year, gender, and time spent on the Internet). Upon completion of the survey, the respondent was thanked for his/her time. As all participants must take the test at the same time, a debriefing statement (as per the Psych Pool requirements) was administered when all participants have finished.

4. Results and Discussion

4.1 Demographics

With the methods in place, I now discuss the results of my experiment. In total, there were 45 participants over the course of seven sessions. Of the 45, there were 26 males (57.8%) and 19 females (42.2%) who participated. This reflects the general population of Worcester Polytechnic Institute (WPI) and the Psych Pool. In total, there were 15 freshmen (33.3%), 14 sophomores (31.1%), 12 juniors (26.7%) and 4 seniors (8.9%). These results gives a fairly even spread over class years. Finally, 34 of the 45 participants spent more than three hours on the Internet daily. This demographic reflects how integrated Internet usage is in student life. These results are summarized in the following pie charts, Figure 2.

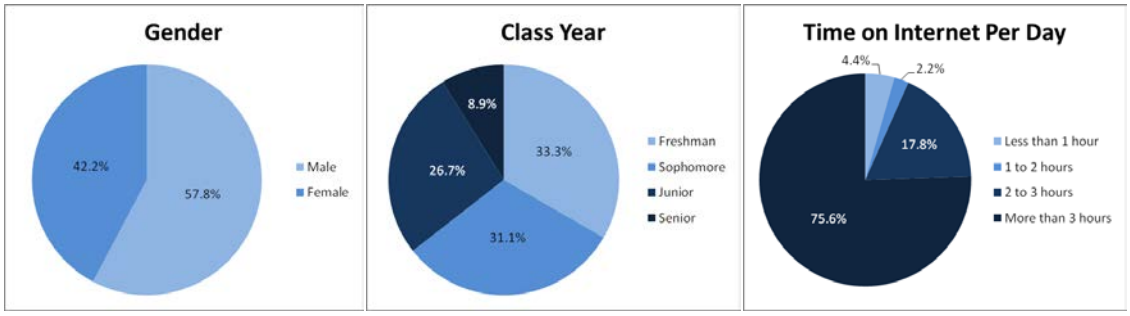

Figure 2: Demographic Information

4.2 Overall Statistics

The following are the results of the Privacy Aptitude Test, shown on a behavior score versus knowledge score graph, Figure 3. The blue data points correspond to individual scores, while the red point is the average score. Finally, a linear curve is fit to the data. Please remember that behavior and knowledge were scored from -1 to 1, where the higher the knowledge score, the more knowledge of Internet privacy a participant

exhibited, while a higher behavior score indicates lower risk behavior of the participant. A zero knowledge score indicates that the participant got 50% of questions correct.

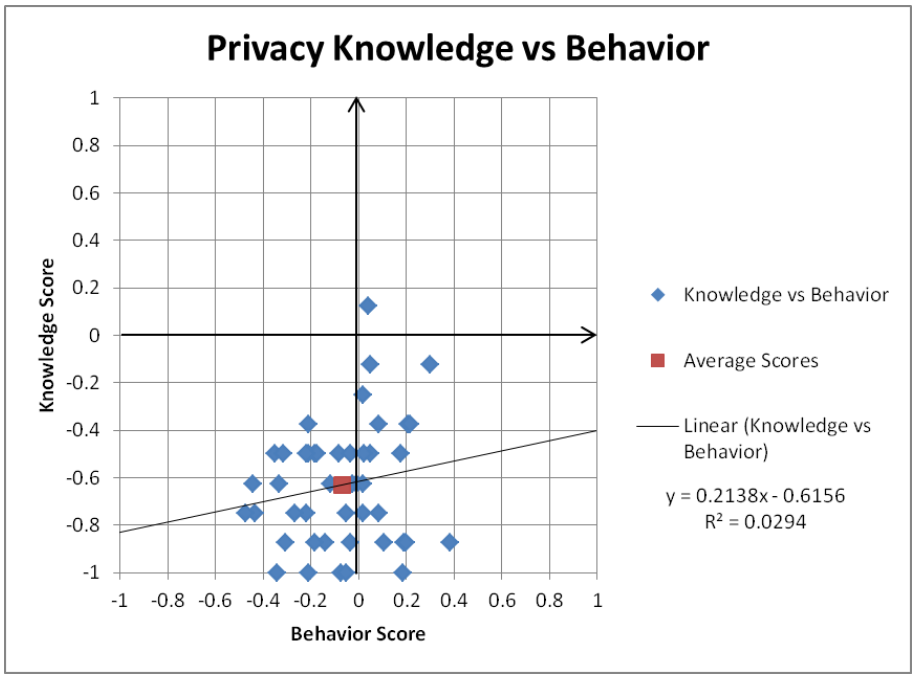

Figure 3: Privacy Knowledge vs Behavior

The average knowledge score was -0.631 (roughly 3 out of 16 questions correct), with a standard deviation of 0.258, while the average behavior score was -0.069, with a standard deviation of 0.207. We observe from Figure 2 that there is a fairly large spread of data. However, it is interesting to note that the data clusters towards a mean of 0 behavior, and a poor level of knowledge. Overall, though, there is a slight increasing trend to the data. Those who scored well on the knowledge test tended to have positive behavior scores, and those who scored very low on the knowledge test did not have high behavior scores. This confirms my research question of whether knowledge of privacy issues will affect a user's behavior.

It is interesting to study what results screen the users visited during the survey. As mentioned in Procedure, to personalize the outcomes, participants were taken to one of

nine screens, corresponding to low (-1 to -0.33), middle (-0.33 to 0.33) and high (0.33, 1) behavior and knowledge scores. Overall, 6 participants saw Screen 1 (low knowledge score, low behavior score), 34 saw Screen 2 (low knowledge score, middle behavior score), 1 saw Screen 3 (low knowledge score, high behavior score) and 4 saw Screen 5 (middle knowledge score, middle behavior score). This data is summarized in the following, Table 3.

		Behavior Range		
		-1 to -0.33	**-0.33 to 0.33**	**0.33 to 1**
Knowledge Range	**0.33 to 1**	**Screen 7** 0 Participants	**Screen 8** 0 Participants	**Screen 9** 0 Participants
	-0.33 to 0.33	**Screen 4** 0 Participants	**Screen 5** 4 Participants	**Screen 6** 0 Participants
	-1 to -0.33	**Screen 1** 6 Participants	**Screen 2** 34 Participants	**Screen 3** 1 Participant

Table 3: Score Range Frequencies

I also analyzed the PAT scores of the demographic subgroups. The average (knowledge score, behavior score) of male participants was (-0.582, -0.086), and that of female participants was (-0.697, -0.047). It is interesting that males knew more on average, but females had higher behavior scores. This can potentially be explained by the fact that males have a higher interest in technology (as indicated by the more male-dominated fields of Computer Science and Electrical Engineering). Females, on the other hand, also may have greater pressure from social norms. For example, a female who exposes herself in a negative manner may be ridiculed by her peers, while the same is not

the case for males. This would lead to females being more cautious on the Internet (particularly in a social network setting).

In class year subgroups, freshmen had scores of (-0.608, 0.00044), sophomores scored (-0.741, -0.222), juniors scored (-0.615, 0.00219) and seniors (-0.375, 0.00217). There does not seem to be an explanation as to why sophomores knew the least knowledge questions (or why seniors knew the most). However, it is interesting how sophomores also scored the worst on average. To see if class year had any effect on scores, it would be necessary to collect additional data.

Finally, I analyzed the effects of time on the Internet and privacy scores. Participants who spent less than 3 hours on the Internet per day had average scores of (-0.659, -0.052), and those who spent more than 3 hours per day had average scores (-0.621, -0.075). Again, time on the Internet does not seem to have much effect on privacy scores.

These statistics are summarized in the following, Figure 4. Please note that the graph only represents a partial description of the full graph (Figure 3). All subsequent knowledge-behavior graphs will also only show a portion of the overall graph.

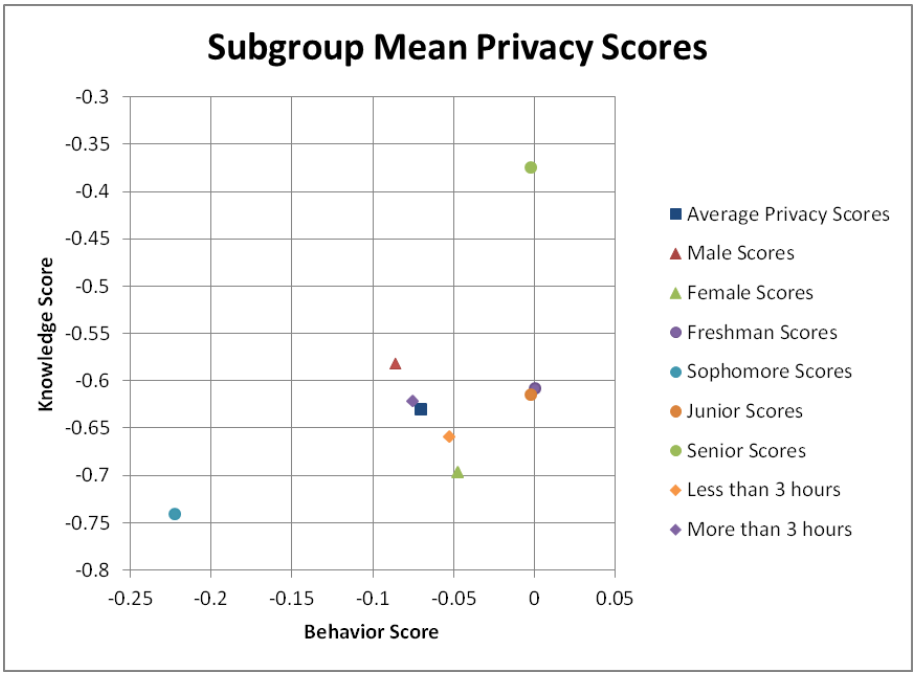

Figure 4: Subgroup Mean Privacy Scores

4.3 Personality Test Results

To test my second question, I gave the participants the Ten Item Personality Inventory (TIPI), which tests participant's Big Five Factor personality types. However, instead of the factor Neuroticism, TIPI tests for Emotional Stability (in essence, the opposite of Neuroticism). Each question was scored from 1 to 7 on a Likert-scale, and questions were scored as per the original test. Thus, scores for each personality type could range from 6 to 42. Figure 5 below shows the average response to each question, as well as the overall average.

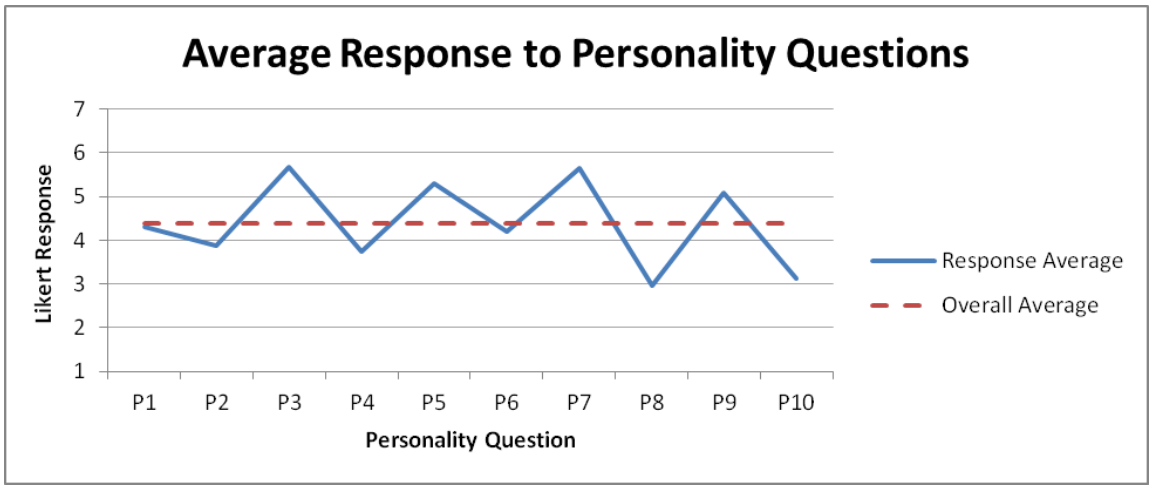

Figure 5: Average Response to Personality Questions

We observe that the average response is very close to 4 (the median Likert-Scale Response). This means that the test worked well accurately gauging responses. It is of note that questions 2, 4, 6, 8 and 10 are all below average while questions 3, 5, 7 and 9. This is due to the fact that the personality adjectives given in the even numbered questions were negative qualities, such as "critical" or "careless." It is expected that people would rate themselves lower for negative qualities and higher for positive qualities, such as "dependable" or "sympathetic."

Overall, the average scores for each personality type are as follows, Table 4.

Personality Type	Mean Score
Extraversion	27.49
Agreeableness	28.82
Conscientiousness	29.73
Emotional Stability	29.16
Openness	28.02

Table 4: Mean Personality Type Scores

To analyze the effects of personality on privacy scores, I looked at participants whose personality inventories were higher than the mean. This means that an individual with an Extraversion score higher than 27.49 would be considered high in Extraversion, etc. I also tested to see if gender subgroups of personality types had any effect on scores.

The mean scores of those high in Extraversion were (-0.644, -0.100), while extraverted males scored (-0.575, -0.102) and extraverted females scored (-0.713, -0.098). We see that extraverted participants had slightly worse knowledge scores, but significantly worse behavior scores (roughly a factor of 0.04). This could be attributed to the fact that extraverted individuals would be more likely to share more information about themselves than those who are not extraverted. Meanwhile, the male/female subgroups exhibited the same results as for the entire population.

Those high in Agreeableness scored (-0.630, -0.096). Agreeable males scored (-0.571, -0.094), and agreeable females scored (-0.713, -0.098). Like Extraversion, agreeable participants had worse behavior scores, but exhibited slightly better knowledge scores. Interestingly, agreeable females scored worse than their male counterparts in terms of both knowledge and behavior.

Conscientious individuals averaged scores of (-0.661, -0.077). Conscientious males scored (-0.563, -0.105), and conscientious females scored (-0.750, -0.051). It is interesting that conscientious individuals on average did not score too much worse than average. However, conscientious males, while more knowledgeable, had scores rivaling that of the extraverts. One would normally expect conscientious individuals to be more cautious of privacy issues (and would adjust their behavior accordingly). However, my results indicate that males do the opposite.

The mean scores of emotionally stable participants were (-0.645, -0.096), while males scored (-0.525, -0.119), and females scored (-0.778, -0.069). Emotionally females had worse knowledge scores, but their behavior was nearly average. Emotionally stable males, on the other hand, had the worst average behavior scores. Why is this so?

Emotional Stability is the opposite of Neuroticism. A neurotic individual would perhaps be more paranoid about Internet privacy, and would therefore protect their personal information online. If Emotional Stability is truly the opposite of Neuroticism, then perhaps emotionally stable individuals would not be as paranoid, and therefore not exhibit the same level of privacy concerns.

Individuals high in Openness scored (-0.719, -0.075), with males scoring (-0.667, -0.063), and females scoring (-0.761, -0.086). Open individuals scored worse than average; however, we do not observe the erratic scores of the other personality types. Perhaps there is not much correlation between Openness and privacy scores.

The average privacy scores of those high in a particular personality type, shown with the overall mean of the entire test population, are represented on the graph below, Figure 6.

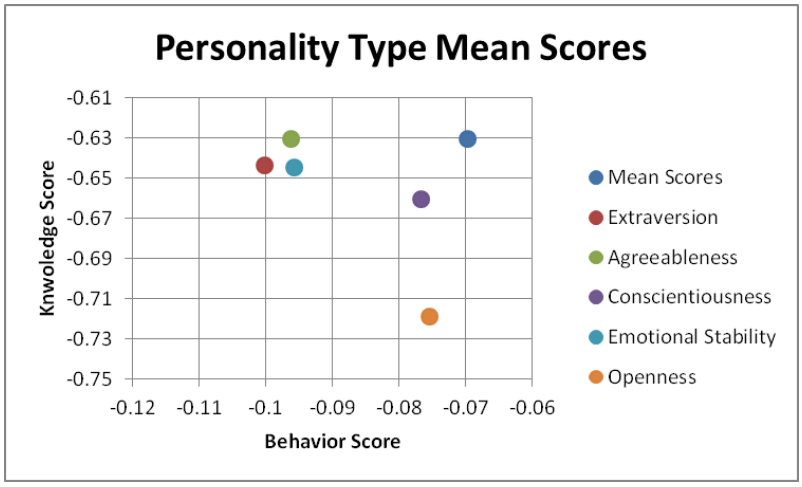

Figure 6: Personality Type Mean Scores

We observe that every personality type scored worse than the mean (except Agreeableness, which had a mean knowledge that was slightly greater than the mean). While the scores are overall worse than average, we see that certain personality types affect one score more than the other. Extraversion, Agreeableness and Emotional

Stability all have knowledge scores that are nearly equal (or only a little off) from the mean, but worse behavior scores. Extraverts are probably more likely to show more of themselves online. Agreeable individuals may want to get along with their friends, and will not use as safe privacy practices online. Emotionally stable individuals, unlike their opposite, neurotic individuals, might not care as much about Internet privacy practice. On the other hand, conscientious and open individuals had behavior scores rivaling the mean, yet have lower knowledge scores. In general, those high in Conscientiousness have the closest scores to the mean. There is no explanation within personality types as to why certain personalities had higher or lower knowledge scores than the others. This is most likely attributed to population anomalies (the specific population tested).

Figure 7 below shows the behavior scores for individual personality types, as well as those for males and females. For reference is the mean behavior score of the entire test population.

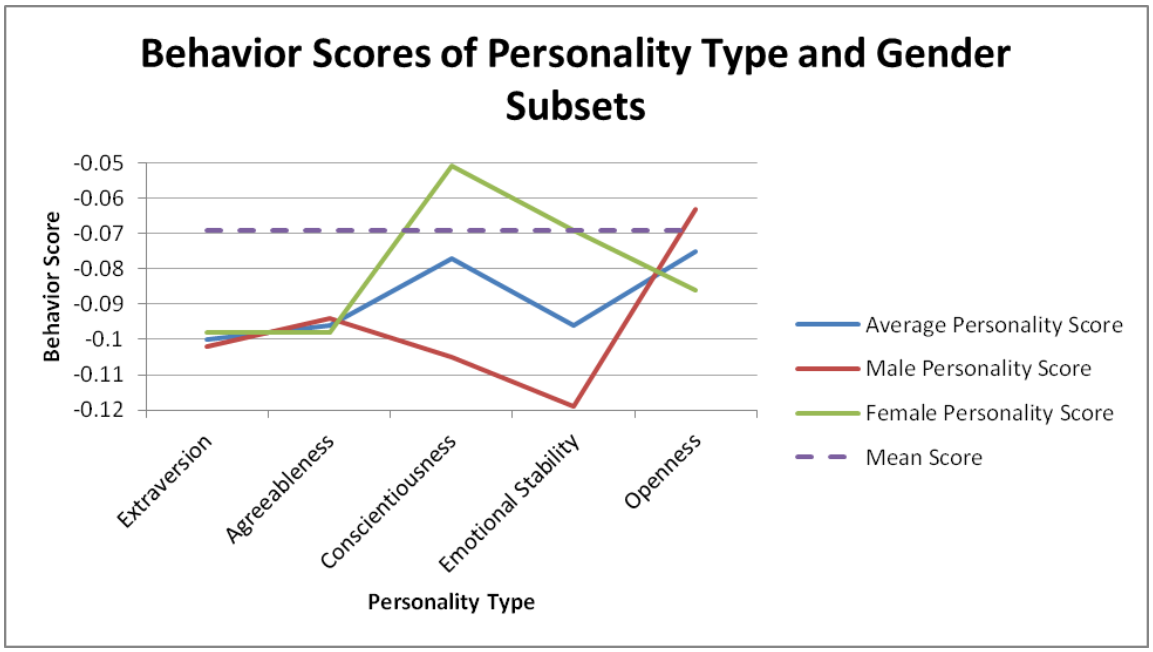

Figure 7: Behavior Scores of Personality Type and Gender Subsets

We observe that, while the average behavior scores for personality types were less than the mean, that some subgroups scored higher. Specifically, conscientious and emotionally stable females scored as well as or greater than the mean. It is further interesting to note that Extraversion and Agreeableness exhibit very little differences for specific genders, while Conscientiousness and Emotional Stability have large deviations.

4.4 Behavior and Knowledge Exam Statistics

The response statistics to each question of the Behavior and Knowledge Exam (PAT) can be seen in Appendix B. There are some points of interest in this response data. Interestingly enough, not every respondent had a social networking profile (only 40 of the 45 did). And, one individual did not have his/her real name on his/her profile. The most common items on an individual's profile page were (in order of percentage): Images or Videos of Myself, My Real Name, Schooling or Employment History, Hobbies and Interests, Date of Birth, and Electronic Contact Information. Also interesting is that 87.5% of respondents' either had pages that could be found via a search engine, or were unsure of whether their profiles could be found on search engine. This particularly comes into play when a potential employer is performing a background check on a potential employee. The employer will most likely check for the individual using a search engine.

As a subset of the data, those who had social networking profiles had average scores of (-0.631, -0.0863), while those who did not scored (-0.625, 0.0633). This means that those without profiles had significantly better behavior (most likely due to the fact that they did not have quantities of information about themselves on SNS). The average knowledge score, however, was roughly the same in both cases.

The knowledge test showed interesting results as well. First, the option of "Do not know" was used with some frequency (used on average by 42.4% of respondents on any given question, or approximately 19 out of 45 respondents). Most questions saw splits in answers. Only a few questions had an option that no one selected. This means that the questions themselves were well prepared. The questions where certain answers were not selected will need to be improved.

All but one knowledge question had at some correct responses, shown below in Figure 8. Only question 2 did not. It is interesting to see that not one of the participants knew how long their IP address is attached to a Google search before being anonymized. This perhaps ties into the fact that only 4.4% of respondents read website privacy policies.

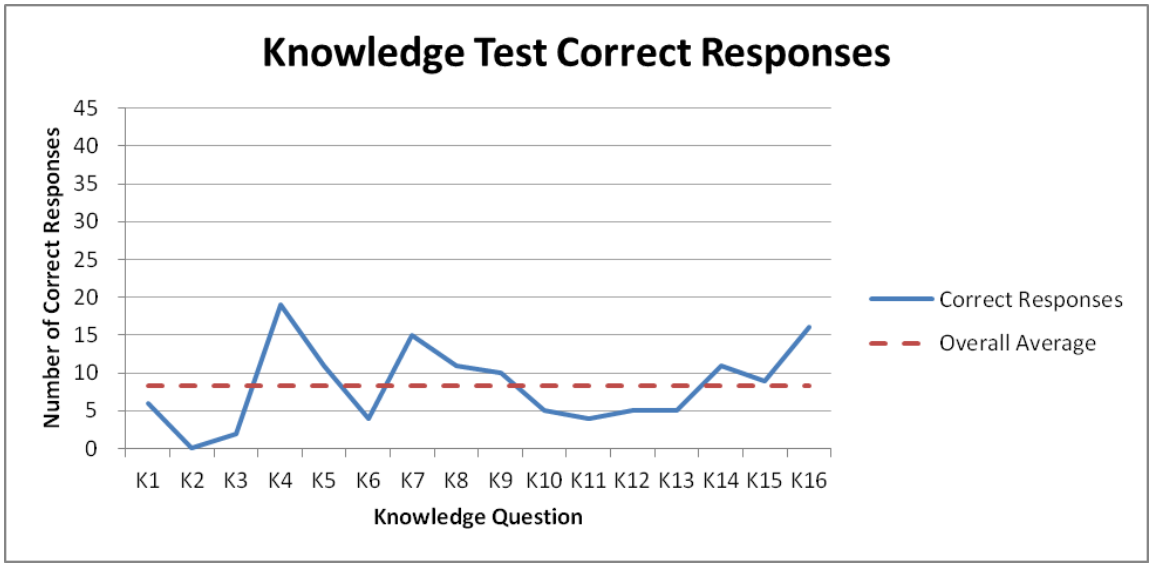

Figure 8: Knowledge Test Correct Responses

Overall, we see that the knowledge test had a very low mean number of correct responses. It is ideal for the responses to tend to 50% correct on any given question. Thus, the knowledge test needs improvement to achieve a more ideal distribution.

While not shown, question 17 had the most correct responses, though only three of the six answers were chosen. This means that the question would not have been effective in gauging privacy knowledge had it been scored.

4.5 Post-Questionnaire Results

The response statistics to the Post-Questionnaire are given in Appendix C. We can analyze the privacy scores of certain responses. Those who indicated that they knew more than expected had scores of (-0.333, 0.031), while those who knew less scored (-0.619, -0.108), and those who knew as expected scored (-0.688, -0.043). Thus, those who indicated they knew more than expected had overall greater knowledge scores. Those who knew less and knew as expected had scores near the average. Satisfaction with ones scores did not indicate any trends in terms of privacy knowledge, though showed some differences in behavior. Those who were satisfied scored (-0.625, 0.015), and those who were not satisfied scored (-0.633, -0.100). Finally, those who were interested in how to change their behavior to better protect their privacy scored (-0.652, -0.071) and those who were not interested scored (-0.573, -0.067). Those who wanted to improve their behavior scored worse than average in both categories, while the reverse holds true for those who did not.

5 Conclusions

In conclusion, the Privacy Aptitude Test (PAT) was a success. I created a surveying tool to score an individual's behavior and knowledge of privacy issues. I found that user behavior scores tended toward zero (neither risky nor cautious), while knowledge scores were not good (on average 3 out of 16 questions correct). This means that users tend to protect their privacy in some regards, but not others. Also, this shows that users do not have a very good understanding of privacy issues or topics. Considering how often people use the Internet, this is an area of great concern.

Furthermore, it is worth noting that the participants in the survey were college students at the Worcester Polytechnic Institute, a school with emphasis on science and technology. As a result, I expect the scores to be better than if I had sampled a random population. In general, youths are more familiar with technology than their elders, meaning that they know more about how technology operates. This means that if WPI students scored 3 out of 16 correct on the knowledge test, then the average of a general population would likely be worse.

Overall, there was a small positive relationship between an individual's knowledge of privacy issues and his/her behavior. In investigating personality types, it was found that personality had some indication on privacy scores, particularly certain personality types affecting behavior scores. Other factors, such as gender, class year, and average time on Internet did have some effect on scores.

5.1 Assessment of the Study

The survey tool itself seems successful, although there were some flaws in its design. First, I would have changed the scoring interval from a -1 to 1 range to a 0 to 100%. This means an individual's knowledge would be scored based on percent correct, while behavior would be scored on the percent of riskiness.

Second, I found that the test requires further pre-testing to get greater variation in scores. As the test is now, most scores were in the range of low knowledge and average behavior. Ideally, I would want users to average in the center (average knowledge and average behavior). Specifically, I think that the knowledge test needs work to achieve a better distribution of scores (rather than tending negative).

Third, while z-Tree offered an easy method of coding the survey, it was not the greatest program. Specifically, I think a more personalized test would be beneficial (one where one's score could be shown on a graph, rather than having to hand out graphs to the respondents).

Finally, I also think that the test would benefit from a larger test population. 45 gave good results, and showed trends, but more would perhaps allow for better data.

5.2 Potential Areas for Further Research

The Privacy Aptitude Test only scratched the surface of privacy behavior testing. I think that privacy psychometrics are a useful tool in analyzing behaviors.

Besides knowledge of privacy issues, there are other areas that affect individuals' behavior online. This includes knowledge of risks and consequences of their behavior,

their risk perception (how much risk they associate with privacy breeches, etc.), their awareness of privacy protection strategies, and how likely they are to use said strategies.

Privacy and Internet behavior are all rather individualized issues. Each user will exhibit practices based on a wide variety of experiences and information. This makes privacy research especially difficult, as there is not always a rule to be found. I think that privacy offers an interesting and insightful look into user psychology, and is a necessary field of research for further understanding of how users perceive the risky world of the Internet.

Sources Consulted

Acquisti, A., & Gross, R. (2009). Predicting social security numbers from public data. *Proceedings of the National Academy of Sciences, 106*(27), 10975.

AdBlock plus - add-ons for firefox. Retrieved December, 2010, from https://addons.mozilla.org/en-US/firefox/addon/1865/

Bansal, G., & Zahedi, F. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150.

Basset, J., & Buckley, K. (2010). *An examination of internet privacy in the united states.* (Interactive Qualifying Project Worcester, MA: Worcester Polytechnic Institute.

Bergmann, M. (2009). Testing privacy awareness. *The Future of Identity in the Information Society,* , 237-253.

BetterPrivacy - add-ons for firefox. Retrieved December, 2010, from https://addons.mozilla.org/en-US/firefox/addon/6623/

Bill of rights transcript - the charters of freedom. Retrieved December, 2010, from http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html

Boritz, E., No, W. G., & Sundarraj, R. (2005). Internet privacy research: Framework, review and opportunities. *Waterloo, Ontario, Canada, University of Waterloo,*

Boritz, E., No, W. G., & Sundarraj, R. (2006). Internet privacy: Framework, review and opportunities for future research. Paper presented at the *Available at SSRN: Http://ssrn. com/abstract, , 908647*

Bradlow, E. T., Hoch, S. J., & Wesley Hutchinson, J. (2002). An assessment of basic computer proficiency among active internet users: Test construction, calibration, antecedents and consequences. *Journal of Educational and Behavioral Statistics, 27*(3), 237.

Center for democracy & technology. Retrieved November, 2010, from http://www.cdt.org/

Chen, S. (2010, November 10, 2010). Can facebook get you fired? playing it safe in the social media world. *CN,* Retrieved from http://www.cnn.com/2010/LIVING/11/10/facebook.fired.social.media.etiquette/index.html?hpt=T2

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108.

Dommeyer, C. J., & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing, 17*(2), 34-51.

Electronic privacy information center. Retrieved November, 2010, from http://epic.org/

Facebook privacy - electronic privacy information center. Retrieved December, 2010, from http://epic.org/privacy/facebook/

Federal trade commision. Retrieved November, 2010, from http://ftc.gov/

Federal trade commission - 2006 identity theft survey report. (2007). Retrieved December, 2010, from http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

Friberg, Å. (2007). *An empirical evaluation of online privacy concerns with a special focus on the importance of information transparency and personality traits* Citeseer.

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

Korzaan, M., Brooks, N., & Greer, T.DEMYSTIFYING PERSONALITY AND PRIVACY: AN EMPIRICAL INVESTIGATION INTO ANTECEDENTS OF CONCERNS FOR INFORMATION PRIVACY.

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems, 48*(4), 15-24.

Lilienfeld, S. O., Lynn, S. J., Namy, L. L., & Woolf, N. J. (2009). *Psychology: From inquiry to understanding* (Second Edition, Examination Copy ed.). Boston: Allyn and Bacon.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs, 38*(2), 217-232.

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. Paper presented at the *Security and Privacy, 2008. SP 2008. IEEE Symposium on,* 111-125.

NoScript - add-ons for firefox. Retrieved 2010, 2010, from https://addons.mozilla.org/en-US/firefox/addon/722/

Online privacy: Using the internet safely - privacy rights clearinghouse. (2010). Retrieved December, 2010, from http://www.privacyrights.org/fs/fs18-cyb.htm

Online shopping tips: E-commerce and you - privacy rights clearinghouse. (2010). Retrieved December, 2010, from http://www.privacyrights.org/fs/fs23-shopping.htm

Orchard, L. J., & Fullwood, C. (2010). Current perspectives on personality and internet use. *Social Science Computer Review, 28*(2), 155.

Ping An Wang. (2010). Information security knowledge and behavior: An adapted model of technology acceptance. Paper presented at the *Education Technology and Computer (ICETC), 2010 2nd International Conference on, , 2* V2-364-V2-367.

Plocienniczak, M. (2010, November 10, 2010). Labor board: Facebook vent against supervisor not grounds for firing. *CNN,* Retrieved from http://www.cnn.com/2010/TECH/social.media/11/09/facebook.firing/index.html?iref=obnetwork

Ponemon, L. (2010). *Concerns about new airport screening procedures.*Ponemon Institute.

Ponemon, L. (2010). *National survey on identity & privacy in social media.*Ponemon Institute.

A primer on behavioral advertising - center for democracy & technology. (2008). Retrieved December, 2010, from http://www.cdt.org/policy/primer-behavioral-advertising

The privacy act of 1974 - electronic privacy information center. Retrieved December, 2010, from http://epic.org/privacy/1974act/

Privacy rights clearinghouse. Retrieved November, 2010, from http://www.privacyrights.org/

Private browsing - firefox help. Retrieved December, 2010, from http://support.mozilla.com/en-US/kb/Private%20Browsing

Re-identification - electronic privacy information center. Retrieved December, 2010, from http://epic.org/privacy/reidentification/

Rosen, J. (2010, July 21). The web means the end of forgetting. *New York Times,*

Social networking privacy: How to be safe, secure, and social - privacy rights clearinghouse. (2010). Retrieved December, 2010, from http://www.privacyrights.org/social-networking-privacy

Torkzadeh, G., & Van Dyke, T. P. (2002). Effects of training on internet self-efficacy and computer user attitudes. *Computers in Human Behavior, 18*(5), 479-494.

Van Dyke, T. P. (2009). Ignorance is bliss: The effect of increased knowledge on privacy concerns and internet shopping site personalization preferences. In H. Nemati (Ed.), *Techniques and applications of for advanced information privacy and security: Emerging organizational, ethical, and human issues* (pp. 225-226-243). Hershey, PA: Information Science Reference.

Wills, C. E., & Zeljkovic, M. (2010). *A personalized approach to web privacy - awareness, attitudes and actions.* Unpublished manuscript. Retrieved November, 2010, from http://web.cs.wpi.edu/~cew/tmp/final.pdf

Wyatt, E., & Vega, T. (2010, F.T.C. backs plan to honor privacy of online users. *New York Times,*

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology, 58*(5), 710-

Appendix A. Behavior Exam Scoring Rubric

General Browsing Habits

1. How often do you delete cookies?
    a. Never -1
    b. At least once a month -0.67
    c. Every week -0.33
    d. Every few days +0.33
    e. Every day +0.67
    f. After every browsing session +1
2. Do you use ad-blocking tools or add-ons with your Internet browser?
    a. Yes +1
    b. No -1
3. Do you use private browsing options with your Internet browser?
    a. Yes +1
    b. No -1
4. Do you use spyware and anti-virus protection software?
    a. Yes +1.5
    b. No -1.5
5. Do you…?
    a. Allow cookies only from sites I visit +0
    b. Allow all cookies -1
    c. Block all cookies +1
6. Do you read the privacy policies of websites you visit?
    a. Yes +1
    b. No -1
7. Do you encrypt your IP address?
    a. Yes +1
    b. No -1
8. Do you use encryption for email or hard disk protection?
    a. Yes +1
    b. No -1
9. Do you ever visit websites with which you are unfamiliar?
    a. Yes -0.5
    b. No +0.5

Social Networking Habits

1. Do you have a profile on a social networking site? [This question does not assign a score but filter whether or not the respondent will answer the next four questions. In any case, the neutrality of the test is preserved. Furthermore, answering "No" gives a score of 0 to the next four questions]
    a. Yes +0
    b. No +0
2. What information about yourself do you have on your profile? (Check all that apply) [Default score is +1. For each checked, -1/6. This yields a -1 if all are checked]

a. Your real name
b. Images or videos of yourself
c. Electronic contact information (email address, IM screen name)
d. Phone number
e. Home Address
f. Age
g. Date of Birth
h. Schooling or employment history
i. Political views
j. Religious views
k. Sexual Orientation
l. Hobbies or interests

3. Who can view your profile?
   a. Only friends +1
   b. Friends and Network +0
   c. Anyone -1
4. Can someone find your profile using a search engine?
   a. Yes -1
   b. No +1
   c. Don't Know -1
5. Do you allow third-party applications to have access to your profile?
   a. Yes -1
   b. No +1
6. Have you ever used location-based services, examples include position-fixing features of Facebook Places or Foursquare or GPS?
   a. Yes -1
   b. No +1

E-Commerce Habits

1. How often do you shop online?
   a. Rarely +1
   b. Infrequently +0.33
   c. Frequently -0.33
   d. Very frequently -1
2. Have you ever made a purchase from a seller outside the U.S.?
   a. Yes -1
   b. No +1
3. When visiting a website, do you check for TRUSTe, Verisign, or BBBonline seals-of-approval?
   a. Yes +1
   b. No -1
4. How do you pay for purchases online? (Check all that apply)
   a. Credit card +1
   b. Debit or ATM card +0
   c. Check or money order -1
   d. Money transfer -1

e. Paypal +1

5. Have you ever disclosed your Social Security Number online?

a. Yes -1

b. No +1

6. When creating an account on a website or giving billing or shipping information to online stores, have you ever provided information marked “Optional”?

a. Yes -1

b. No +1

Appendix B. Behavior Exam and Knowledge Exam Response Statistics

Behavior Exam

General Browsing Habits

1. How often do you delete cookies?
    a. Never 46.7%
    b. At least once a month 28.9%
    c. Every week 8.9%
    d. Every few days 6.7%
    e. Every day 0.0%
    f. After every browsing session 8.9%
2. Do you use ad-blocking tools or add-ons with your Internet browser?
    a. Yes 80.0%
    b. No 20.0%
3. Do you use private browsing options with your Internet browser?
    a. Yes 44.4%
    b. No 55.6%
4. Do you use spyware and anti-virus protection software?
    a. Yes 86.7%
    b. No 13.3%
5. Do you…?
    a. Allow cookies only from sites I visit 51.1%
    b. Allow all cookies 35.6%
    c. Block all cookies 13.3%
6. Do you read the privacy policies of websites you visit?
    a. Yes 4.4%
    b. No 95.6%
7. Do you encrypt your IP address?
    a. Yes 2.2%
    b. No 97.8%
8. Do you use encryption for email or hard disk protection?
    a. Yes 15.6%
    b. No 84.4%
9. Do you ever visit websites with which you are unfamiliar?
    a. Yes 88.9%
    b. No 11.1%

Social Networking Habits

1. Do you have a profile on a social networking site?
    a. Yes 88.9%
    b. No 11.1%

[The following statistics for questions 2, 3, 4 and 5 are the percentages for those 40 participants who do have social networking profiles]

2. What information about yourself do you have on your profile? (Check all that apply)

a. Your real name	97.5%
b. Images or videos of yourself	100%
c. Electronic contact information (email address, IM screen name)	80.0%
d. Phone number	20.0%
e. Home Address	7.5%
f. Age	70.0%
g. Date of Birth	82.5%
h. Schooling or employment history	97.5%
i. Political views	35.0%
j. Religious views	40.0%
k. Sexual Orientation	80.0%
l. Hobbies or interests	85.0%

3. Who can view your profile?

a. Only friends	60.0%
b. Friends and Network	25.0%
c. Anyone	15.0%

4. Can someone find your profile using a search engine?

a. Yes	40.0%
b. No	12.5%
c. Don't Know	47.5%

5. Do you allow third-party applications to have access to your profile?

a. Yes	22.5%
b. No	77.5%

6. Have you ever used location-based services, examples include position-fixing features of Facebook Places or Foursquare or GPS?

a. Yes	35.0%
b. No	65.0%

E-Commerce Habits

1. How often do you shop online?

a. Rarely	15.6%
b. Infrequently	44.4%
c. Frequently	24.4%
d. Very frequently	15.6%

2. Have you ever made a purchase from a seller outside the U.S.?

a. Yes	57.8%
b. No	42.2%

3. When visiting a website, do you check for TRUSTe, Verisign, or BBBonline seals-of-approval?

a. Yes	37.8%
b. No	62.2%

4. How do you pay for purchases online? (Check all that apply)

a. Credit card	35.6%
b. Debit or ATM card	46.7%
c. Check or money order	0.0%

d. Money transfer	0.0%
e. Paypal	17.8%

5. Have you ever disclosed your Social Security Number online?

a. Yes	35.6%
b. No	64.4%

6. When creating an account on a website or giving billing or shipping information to online stores, have you ever provided information marked "Optional"?

a. Yes	33.3%
b. No	66.7%

Knowledge Exam

* Indicates the correct response

1. Which of the following is **not** Personally Identifiable Information (PII)?

a. Name	2.2%
b. Address	4.4%
c. Social Security Number	2.2%
d. Date of Birth*	13.3%
e. All of the above are considered PII	53.3%
f. Do not know	24.4%

2. How long is your IP address attached to a search on Google.com?

a. 3 month	0.0%
b. 6 months	2.2%
c. 9 months*	0.0%
d. 1 year	2.2%
e. Forever	4.4%
f. Do not know	91.1%

3. Which of the following online payment methods is considered the most secure?

a. Credit card*	4.4%
b. Debit or ATM card	6.7%
c. Check or money order	4.4%
d. Money transfer	0.0%
e. PayPal	44.4%
f. Do not know	40.0%

4. When you deactivate an account on Facebook.com, what information does the website delete? Consider the following:

I. Personal Information (Name, address, date of birth)
II. Uploaded media (photos, videos, taggings)
III. User posts

a. I and II	4.4%
b. I and III	0.0%
c. I, II, and III	11.1%
d. Nothing is deleted*	42.2%
e. Do not know	42.2%

5. What does private browsing do?

a. Cookies are not downloaded onto your computer's browser	2.2%
b. Website history is not captured by online marketers	4.4%
c. Your website history is not stored on your computer*	24.4%
d. Your computer's IP address is not collected on websites you visit	2.2%
e. Do not know	66.7%

6. Which of the following is not the type of information typically used by behavioral advertisers to target you when using the Internet?

a. Recent websites visited	11.1%
b. Website registration information*	8.9%
c. Recent online purchases	2.2%
d. Planned future purchases	24.4%
e. Search queries	6.7%
f. Do not know	46.7%

7. When visiting a website you see a seal such as TRUSTe, Verisign or BBBonline somewhere near the merchant's privacy policy or home page. What does this mean?

a. The website does not collect your personally identifiable information	0.0%
b. The website does not sell or share your personal information	22.2%
c. The website does not retain your personal information	2.2%
d. The website meets reasonable privacy standards*	33.3%
e. None of the above	0.0%
f. Do not know	42.2%

8. The Children's Online Privacy Protection Act attempts to protect children from online abuses. What is the age that defines a child for purposes of compliance with this US federal act?

a. Less than 21 years of age	0.0%
b. Less than 18 years of age	37.8%
c. Less than 13 years of age*	24.4%
d. Less than 10 years of age	0.0%
e. Do not know	37.8%

9. In the context of control over your personal information with an online merchant, what does the term "opt out" mean?

a. Never use my personal information for any reason 6.7%
b. Never sell my personal information 0.0%
c. Never share my personal information 4.4%
d. Never retain my personal information 0.0%
e. All of the above 11.1%
f. It depends on the merchant* 22.2%
g. Do not know 55.6%

10. Which one of the following is **not** considered public information?

a. Your home's assessed value 4.4%
b. Your real estate tax bill 0.0%
c. Your income tax return* 11.1%
d. Your court records 15.6%
e. All of the above are public records 35.6%
f. Do not know 33.3%

11. In terms of US privacy protections, what is considered an illegal act?

a. Company tracks your behavior online without letting you know 0.0%
b. Company sells your information without your consent 24.4%
c. Company uses information about you that is known to be incorrect or inaccurate 2.2%
d. Company does not give you a choice in how your information will be used 2.2%
e. All of the above are illegal acts 37.8%
f. None of the above is an illegal act* 8.9%
g. Do not know 24.4%

12. With respect to individual privacy rights, what statement is most likely to be true?

a. US provides more individual privacy rights than most other countries 15.6%
b. EU nations provide more individual privacy rights than the US 4.4%
c. EU and US privacy rights are about the same 4.4%
d. US is considered one of the worst nations for individual privacy rights* 11.1%
e. None of the above 0.0%
f. Do not know 64.4%

13. In terms of privacy protections, what statement is true about your computer's IP address?

a. IP address is always considered personally identifiable information 22.2%
b. IP address is never considered personally identification information 2.2%
c. The IP address on your device can never be faked or manipulated 4.4%

d. None of the above are true* 11.1%
e. Do not know 60.0%

14. What statement is true about the use of your Social Security Number for purposes of individual identification?

a. The SSN can never be used to identify an individual 2.2%
b. The last four digits of the SNN can only be used to identify an individual 20.0%
c. A company cannot post your SSN to machine readable documents or forms 22.2%
d. None of the above statements are true* 24.4%
e. Do not know 31.1%

15. When an online merchant says your personal information will remain completely anonymous, what does that mean?

a. Your personally identifiable information will not be collected or used* 20.0%
b. Your personally identifiable information will not be retained or stored 17.8%
c. No information about you will be collected or used 2.2%
d. No information about you will be retained or stored 11.1%
e. None of the above 20.0%
f. Do not know 28.9%

16. What data element is not typically used to identify and authenticate users?

a. Date of birth 6.7%
b. Email address 8.9%
c. Home address 11.1%
d. Credit card number 20.0%
e. Account number 4.4%
f. All the above are typically used* 35.6%
g. Do not know 13.3%

17. [UNGRADED] Most of what you see on the Internet – such as current news, articles, social networking sites, blogs and wikis – are available free of charge. Who pays for this content you see on the Web? Please check the one response that best defines what you believe.

a. My Internet service provider 6.7%
b. Online advertisers* 75.6%
c. My wireless telephone provider 0.0%
d. Online merchants such as Amazon or eBay 0.0%
e. Government 0.0%
f. Do not know 17.8%

Appendix C. Post-Questionnaire Response Statistics

1. Did you learn anything from the test?
    a. Yes 55.6%
    b. No 44.4%
2. Does the information presented in the test seem startling?
    a. Yes 42.2%
    b. No 57.8%
3. How risky does your behavior seem in relation to your expectations?
[No data exists on this question due to a coding problem in the survey, which prevented the data from this question to be recorded]
    a. Riskier than expected
    b. Less risky than expected
    c. As expected
4. How much did you know about Internet privacy compared to your expectations?
    a. More than expected 6.7%
    b. Less than expected 48.9%
    c. As expected 44.4%
5. Were you satisfied with your scores?
    a. Yes 26.7%
    b. No 73.3%
6. Would you want to take the test again at a future time?
    a. Yes 33.3%
    b. No 66.7%
7. Would you be interested in learning about how to change your behavior to better protect your privacy?
    a. Yes 73.3%
    b. No 26.7%