WORCESTER POLYTECHNIC INSTITUTE

Self-Disclosure on Social Networking Sites

In partial fulfillment of the Interactive Qualifying Project

By Derek Carey

Alexander Misch

Anthony Spencer

Richard Speranza

Advisor

Professor Eleanor Loiacono

Contents

Table of Figures

Table of Tables

Abstract:

This study aims to show that the intention to disclose information is similar but not equivalent to the intention to use social networking sites. Several factors that were not shown to have an impact on intention to use but were shown to have an impact on intention to disclose information were the consumer's emotional stability and agreeableness. Also several factors that have been shown to impact a consumer's perceived risk, perceived benefit, and trust for different scenarios were tested.

Executive Summary:

Given a lack of definitive research regarding habits of consumers on social networking sites, our Interactive Qualifying Project (IQP) team decided to invest in this area. Previous e-commerce research has analyzed the significance variables including perceived benefit, perceived risk, trust, reputation, and personality type on a consumer's intention to use particular electronic businesses. Modifying previous findings, our project team created a theoretical model on how consumers choose to disclose information about themselves on social networking sites. The core of this model consisted of three primary constructs of perceived risk, perceived benefit, and consumer trust which all directly impact a consumer's decision to disclose information. These constructs were comprised of lesser constructs including consumer efficacy, site reputation, perceived privacy, etc. In order to test the accuracy of this model a survey was created based off certified questions from previous research and studies. This survey was distributed to undergraduate students at Worcester Polytechnic Institute (WPI) in Decembers of 2011 with a response rate of 15%. Linear regression analysis in IBM SPSS was carried out in

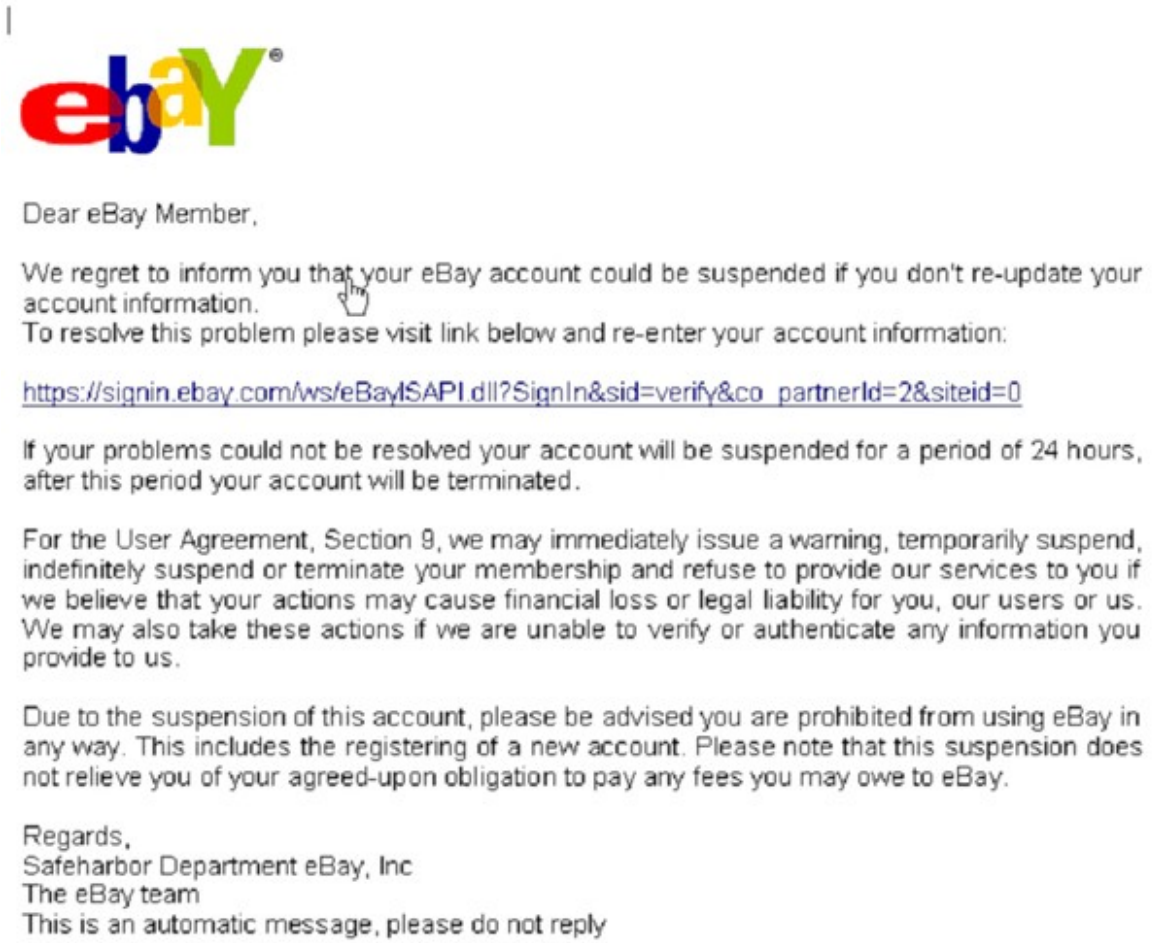
order to determine the validity of our hypotheses. Results confirmed the significance of perceived risk, perceived benefit, and consumer trust on intention to disclose. Additional personality traits such as level of extroversion, emotional stability, and agreeableness were also found to significantly alter consumer disclosure behavior. While most of the hypotheses within the model were statistically significant, there were several instances where components of the model were invalidated for lack of significant support. Interestingly, perceived risk was determined to have a still significant but rather weak effect on self-disclosure. Survey respondents answered questions on intention to disclose information on social networking sites rather than intention to use social networking sites which may have impacted results. Future research on the subject may choose to look further into this phenomenon or the nature of consumer personality type on consumer disclosure behavior on social networking sites. To satisfy IQP requirements of a project with some form of interaction between society and technology, our project team also developed a web site to educate incoming WPI students about social networking and its implications. The website offers information on the history of social networking and includes quizzes, videos, links and additional information on the risks, dangers, expectations, and best practices regarding use of social networking. Facebook is covered in particular detail due to the high prevalence of its use in the collegiate environment. The website will be incorporated into a freshmen residential floor program in future academic years at WPI. It is the hope of the project team that our research and educational efforts should be used and expanded upon in the future to facilitate greater understanding and education on social networking.

Introduction:

Information security continues to be a concern for businesses as Internet based technologies become increasingly prevalent. After several high profile security breaches in 2011 on large companies, such as Lockheed Martin, Sony, Bank of America, and Citigroup, most organizations are reaffirming their commitment to protecting customer data. Stolen information often includes user names, passwords, and even credit card information from online services. Due to the high interconnectivity of information, when personal information from one service is stolen; identity theft and exploitation are common. Users who frequently reuse passwords can open themselves up to multiple attacks, which may result in unauthorized access to personal banking and email accounts.

While security breaches against companies make headlines and represent a significant threat to the livelihood of consumers, direct attacks on individual consumers remains a largely unresolved issue. Social engineering is defined as "The art and science of getting people to comply with your wishes." (Hasan 2010) Social engineering often takes the form of impersonation, trickery, and blackmail when used to attack information systems. In these types of attacks, illegitimate parties or persons typically masquerade as some kind of trusted source such as a system administrator or official in order to collect personal information from unsuspecting consumers. In more sophisticated cases, cyber-criminals may even create seemingly legitimate websites for the purpose of imitating popular businesses or websites. When a customer or user visits these fake pages, these criminals may install malware or steal credit card numbers and other personal information. A growing number of sophisticated tools and resources are available that make social engineering attempts much more believable than in the past. Great coders and web designers can make imitation websites nearly identical to the real

thing. Clever and believable wording can make normally suspicious emails or other correspondence seem legitimate. In many cases, victims are completely unaware of the illegitimate nature of social engineering until it affects their credit, bank accounts, and reputation. Some examples of phishing cases are shown below in Figure 1. The main objective of phishing is to have the consumers submit key personal information like credit card numbers, social security numbers, and login information.



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Figure 1: Two examples of phishing sites asking for personal information taken from http://www.berghel.net/publications/phishing/phishing.php. Note the similarities between these sites and the actual sites they are imitating. The first example is an eBay phishing site asking for personal information. The second example is an imitation website for PayPal to collect information from consumers.

Social engineering is made all the easier with the high degree of personal information the average consumer freely distributes online. The growth of social networks over the past decade has revolutionized the way people communicate, businesses market their products, and consumers learn about new products, services, and trends. However, the average consumer often fails to realize how much the personal information they post online can open them up to targeted attacks. People who “check in” to a restaurant or ballgame on Facebook, Google+, or foursquare let anyone, regardless of intent, know where he or she can be found or when they are away from his or her home. Information on favorite music, birthdates, hobbies, etc. gives thieves an extra edge in guessing passwords or bank security questions. Knowing individual interests also allows dedicated criminals to construct elaborate phishing or social engineering attacks designed with one individual person in mind. When criminals have the possibility of making thousands or even millions of dollars off of one successful attack, the likelihood that any vulnerable person will be targeted is high.

Previous studies have developed and tested theoretical models explaining how and why consumers make a decision to purchase a product online. Factors such a perceived risk, perceived privacy, perceived security, perceived benefit, familiarity, disposition to trust, and intention have all been linked to the a consumers ultimate decision to buy a product online and from a particular site. Little to no research exists that attempts to explain how consumers evaluate the decision to post information on social networking sites or why they ultimately choose to post this sometimes risky information. Our project goal is to develop a trust based decision model on how consumers disclose and distribute personal information on social networking sites. It is our belief that educating consumers on their social behavior on the Internet will allow for more careful evaluation of their actions. Consumer understanding of how they may

be successfully solicited for information may offer valuable insights into how they can take steps to protect themselves in the event that this behavior is unwelcome.

Background:

Social networking sites are very popular websites in today's online market. Millions of consumers of social networking sites visit these sites as a part of their everyday life. Social networking sites are defined as "websites in which consumers setup a personal or professional profile" (**Boyd, 2008**). This profile can be public or semi-public and often contains a list of users with which the consumer has connections. These connections can be shared with other users, and in return, the consumer can see other users' lists of connections (Boyd, 2008). Social networking sites are unique in that not only can consumers meet new people that were once strangers, but also extend their own personal social network online.

The development of social networking sites has followed a trend needing more personal information. This trend started with Six Degrees and has developed into Google +. Figure 2, below, shows a chronological diagram of the different social networking websites that have made major contributions to the development of social networking.

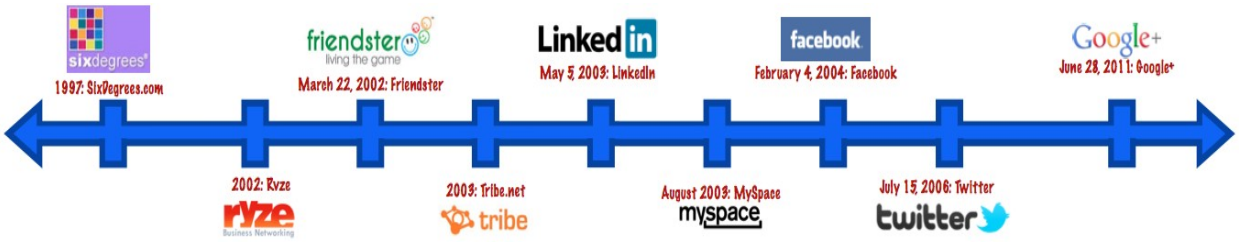


Figure 2: A chronologic timeline of social networking sites

In May 1997, the first social networking site, SixDegrees.com, made its début. It allowed consumers to create profiles and organize connections with others. The site was later modified in

1998 to allow the sharing of these profile and connection lists. This functionality solidified SixDegrees.com as a social networking site. The idea behind SixDegrees.com was to help people stay connected with their friends by sending messages. However, SixDegrees.com was not without its fair share of problems. At the time there was not a large base of people online and the consumers of SixDegrees.com were not able to build a strong network of friends online (Boyd, 2008). Consumers also claimed there was little to do on the website but accept friend requests. Poor business planning coupled with the market downturn of 2000 finalized the end of SixDegrees.com. Even though SixDegrees.com had a short lifespan, its ability to attract millions of consumers foreshadowed the success of future social networking sites to come.

In 2001, a website called Ryze was released. Ryze brought the idea established by SixDegrees.com to the business world. The initial idea was a way for workers to establish social events for businesses in order to help build good business relationships. Ryze quickly expanded into different types of professional activities as well. Ryze allowed users to join different groups called "networks." These networks offered access to a variety of content in the network. The events sponsored by Ryze were often public events. Events sponsored by Ryze were supposed to promote close up and personal interactions between different consumers. Ryze also offered a "Gold" membership to consumers who demanded a higher level of access to information. Although Ryze never acquired massive popularity, its expanded growth demonstrated the importance and value of social networking sites in the online universe (Kiehne, 2004).

One social networking site that had a lot of similarities to Ryze was Tribe.net. Tribe.net offered messaging amongst consumers, user searches, and event listings. Instead of calling their groups of consumers "Networks" like Ryze, Tribe.net referred to groups as tribes. Tribe.net allowed consumers to join multiple Tribes and the site was known to keep the information of a

consumer's personal and professional life separate. This allowed the consumers of the site to decide what information could be viewed publicly depending on certain criteria they specified (Kiehne, 2004). Tribe.net's focus on privacy proved to be a key component to social networking sites.

In 2003, Friendster, initially designed as a dating service, was formed. Friendster had started with the initial idea that a dating service works better when two strangers have a mutual friend in common. When a consumer signed up for the services of Friendster, they had to answer various demographic questions. Consumers were also allowed to add other personal details, including hobbies and photos. To connect to other people, consumers had to send an invitation. If this invitation was accepted, then the two accounts were automatically linked. Friendster also allowed the consumer to search for other people using their name or email address (Kiehne, 2004).

Friendster's popularity grew rapidly. The site encountered social problems in addition to technical problems due to the large increase in consumers. Friendster's rapid expansion caused the servers to fail regularly; it simply could not handle the amount of visitors to the site. The unreliable service of Friendster unsettled many users who expected a more consistent and reliable social networking experience. However, the social disconnect between Friendster and its consumers doomed the website's success. One such disconnect was the issue of fake Friendster accounts. Fake accounts on Friendster were used to promote places, such as schools or bands. Consumers of Friendster saw fake accounts as a useful way to find and connect to other people that had association with that account. Since, Friendster had a privacy policy that would not provide a consumer's information to anyone that was not within four degrees of that consumer

(Boyd, 2008). Consumers found workarounds with fake accounts allowing them ways to see and meet more people online.

Even though fake Friendster accounts were only a minor adaptation of the original idea of Friendster, the company was repulsed by the notion of fake accounts and started deleting them against the opinions of most customers. Friendster's failure to adapt to the consumer's wishes caused its demise and showed that a social networking site must adapt for the consumers to maintain its relevance. Its lack of adaptation to its consumer's needs was its demise, but laid the groundwork for the success of MySpace and other social networking sites.

In 2002, co-founder Reid Hoffman used his living room to start up LinkedIn. By May 5, 2003, LinkedIn was launched. After one month, LinkedIn had a total of 4500 members (LinkedIn 2012). LinkedIn's consumers use LinkedIn to maintain a detail list for contacts within their line of work to use. LinkedIn allows communication, and referrals between a consumer and their contacts. It is this system of referrals, introduction, networking, and professional conversations among consumers that makes LinkedIn the social networking site of the business community (Papcharissi 2009). LinkedIn had a similar privacy setting as Friendster where consumers could only connect to someone if the mutual friend or acquaintance allowed them. However, consumers could also connect with another consumer if they demonstrated that they somehow knew the person. LinkedIn has grown to become the most popular social networking site amongst the business community.

MySpace, established in August of 2003, grew based on its reputation of adapting to the consumers demand. This can be seen in MySpace's support of bands and their fans. MySpace was not initially launched for bands, but after Friendster refused to accept bands MySpace welcomed them. Later in 2004, teenagers started using MySpace, resulting in the company

changing its underage user policy, now allowing teenagers to use MySpace. MySpace's ability to adapt to the consumer's needs allowed it to be one of the most used social networking sites in history (Boyd, 2008).

In early 2004, Mark Zuckerberg launched Facebook as a Harvard-only social networking site. This meant that all Facebook users had to sign up using an email address ending with harvard.edu. Enforcing the need for a specific email address, Facebook was able to keep the site a closed, private community. Facebook soon grew, expanding to other colleges across the United States. However, it still required a collegiate email address to become a member. Soon Facebook converted to a public platform, allowing anyone to join, including high school students. This action gave consumers the ability to make information available only to certain people. Although Facebook allowed anybody to join the site, it maintained the privacy of corporate Facebook networks where consumers needed a genuine email address from that company in order to gain access (Boyd, 2008). Thus, a person would join their corporate network to allow their coworkers exclusive access to their information.

With the expansion of Facebook came the addition of new features that improved the consumer's experience. However, each new feature Facebook released has come with its own complaints and new insecurities. Facebook is unique in comparison to previous social networking sites because it allows developers to make their own applications to run on Facebook. There has been some outrage from consumers because these applications are not developed by Facebook, and require information from the consumer. Similar outrage came from the release of Facebook's "Open Graph" framework. "Open Graph" was designed for a fast way to personalize other websites such as imdb.com and hulu.com. "Open Graph" allows any public information on a consumer to be used by other websites when that consumer is visiting the

website. Because of Open Graph, consumers felt that Facebook was handing out too much consumer information (Cao, 2010). "Open Graph" also put a Facebook like-button on any website that chose to use "Open Graph" so the consumer could connect back to Facebook from that website. Facebook's features are the reason it has such a large consumer base, but it is also the cause of many security concerns; largely the volume of information disclosed by consumers.

Two years later, in July 2006, Twitter was founded. Twitter allows consumers to set up and post any desired topic under 140 characters. These posts are called "tweets". Consumers can also post images. Twitter differs from other social networking sites because consumers can only connect to others in one direction (Kwak 2010). Thus, a consumer can "follow" another consumer without that consumer "following" them back. Twitter has some limitations that other social networking sites do not. Messages posted on Twitter can only be up to 140 characters to allow the "Tweets" to be sent over text message. Twitter is used by consumers to maintain real-time communications with their friends, a feature which makes Twitter one of the most popular social networking websites.

On June 28, 2011, Google launched a social networking site named Google+. Google advertised Google+ as a social networking site that connects you with friends online the same way you connect with those friends offline. Google+'s main attraction is the consumer's ability to organize their friends into circles. These circles allow the consumer to share information with select circles (Google 2011). Google+ also allows consumers to have a video chat up to nine people. These chat sessions, called "Hangouts," allow consumers to join using either a computer or a mobile phone. Google also implemented Google+ into their search engine for any member of Google+. According to Google, a Google+ member can search Google+ and gain information on places or things from their friends and public Google+ posts (Google 2011). This feature

allows consumers to get answers to questions from their friends.

Since the start of social networking sites in 1997 with SixDegrees.com, both the consumers and companies in charge of these sites have changed dramatically. Social networking sites have learned that they need to keep up with the demand and needs of the consumer to stay profitable. Moreover, the consumers have incorporated social networking sites into their everyday lives. This relationship between the social networking sites and the consumers has shown to be a lasting one, yet one with security concerns. Every social networking site has places for the consumer to enter personal information, and social networking sites rely on consumer information to maintain the features demanded by the consumers. The reason a consumer decides to disclose this information is important to their relationship to social networking sites.

Literature Review:

Modern literature relating to consumer interaction in online social environments places significant emphasis on four key variables: perceived risk, consumer trust, perceived benefit, and intention to disclose. These four variables have been proven in previous studies to have the most significant impact on the level of self-disclosure on e-commerce websites and social networks such as MySpace, Facebook, etc. Each of these variables can be broken down into various other components. The final model tested in this experiment had four different components: cognition, experience, affect, and personality. These four components are shown in more detail in Figure 3, below, which shows the final model tested. Perceived risk is a combination of cognition based variables such as perceived risk and perceived privacy. Additionally, degree of social networking self-efficacy also has a weight on perceived risk. Consumer trust is influenced by the affect-based transference of trust. This is to say that other users factor into a consumer's trust. At the same time consumer predisposition to trust has shown to have similar impact. Perceived benefit of social networking is a combination of the reputation of a social network from the consumer perspective as well as the personality type of the user. Emotional, social, or any other value of social networking depends on the typical behavior of those using the services. As such, a combination of consumer cognition, experience, environment, and personality impact intention to disclose, and ultimately, disclosure on a social networking site. The twelve hypotheses comprising our social networking model assume the findings and conclusions of previous research conducted in the field.

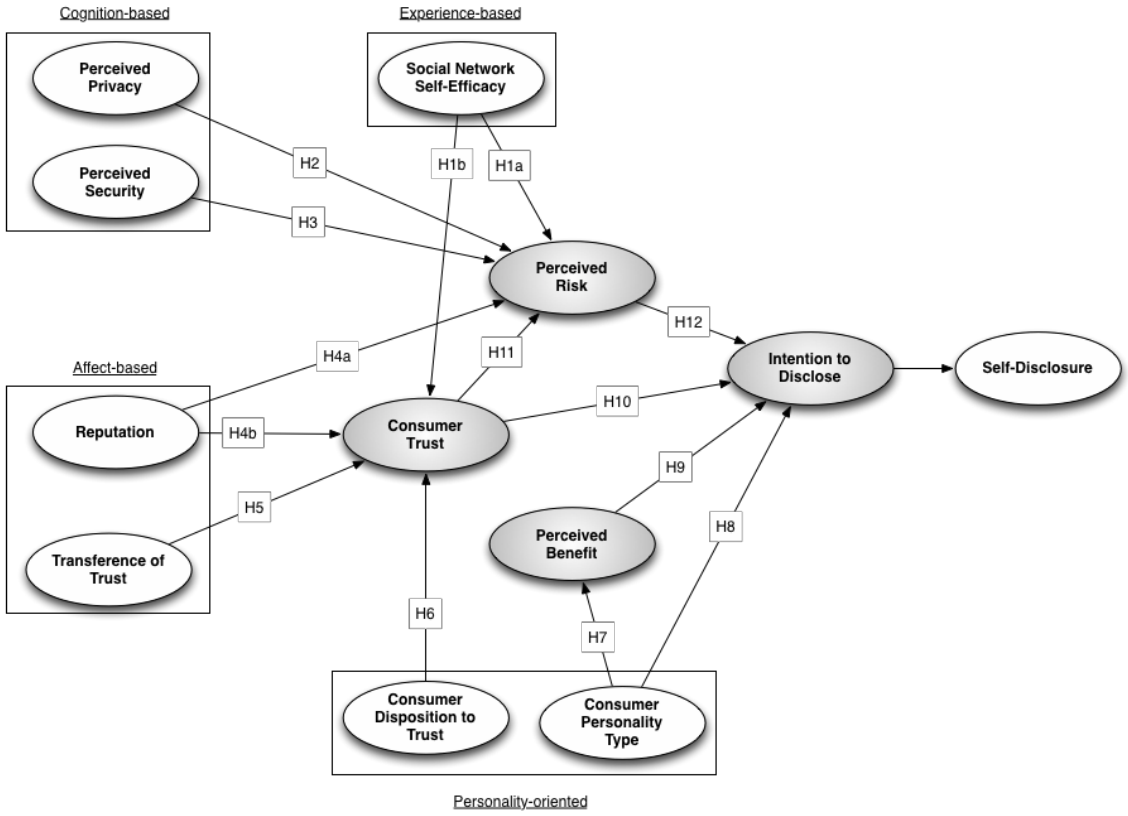


Figure 3: The final breakdown of the model consists of the four major sectors (shown in gray bubbles) and the four components each sector is composed of (shown in white bubbles with black boxes).

Social Networking Self-Efficacy and Perceived Risk:

Self-efficacy is the perceived ability for a person to use his/her knowledge to complete a task. Several measurements are used in self-efficacy including: magnitude, strength, and generalizability. Magnitude denotes the level of difficulty of the task, strength represents the confidence in achieving a task, and generalizability signifies the range of tasks (Compeau, 1995). In terms of trust and risk over the Internet, the consumer's magnitude is the degree of understanding of the website's security, the consumer's strength is the confidence the security will protect information, and the consumer's generalizability is knowledge of a broad range of security methods.

Testing social networking self-efficacy is a relatively new concept, but it is easily adaptable from the testing of computer self-efficacy. In testing computer self-efficacy, the user is

asked to perform a slightly complex task and to rate whether they can complete the task (Compeau, 1995). This test focuses on the magnitude and strength dimensions, however, by repeating the test multiple times with different tasks, the generalization dimension can be found.

Computer self-efficacy can take many forms in the line of social networking. Social networking can take place on sites like Facebook, LinkedIn, and others, but there are several other forms of networking with human-computer interaction. Short message service (SMS) is a widely used form of communication that has taken the place of many face to face or phone call interactions. SMS is very similar to text messaging but it also includes instant messaging services like AOL and Skype. Many of the same factors used to study social networking, e-commerce, and other website interactions are important for SMS. Ease of use, privacy, perceived effectiveness, and subjective norm are all factors in people-to-technology interactions. "The Effectiveness of Short Message Service for Communication with Concerns of Privacy Protection and Conflict Avoidance," a recent article in the Journal of Computer-Mediated Communication, explored these factors for SMS forms of communication. The article used a basic survey method with ratings of 1 to 7 for agreeing or disagreeing with a statement made about SMS. The researcher found that there were strong correlations between SMS and ease of use, privacy protection, and perceived effectiveness (Cho, 2011).

Researchers have found that people are likely to use SMS when communicating private information in crowded areas and are likely to use SMS instead of face-to-face interactions to manage conflicts. Sending private information through SMS could be considered a self-effective task, but the strong ratings of ease of use and perceived effectiveness of SMS are key factors in showing that the users are largely self-effective in SMS technology.

Although some research has shown that being more aware of technology is better at preventing risky behavior, other research has shown the opposite. A study surveying teenagers indicated that there is a positive correlation between risk and self-efficacy (Livingstone, 2010). The survey was conducted on teenagers between the ages of 12 and 17, and it asked them questions about the kinds of websites they visit. As expected, there was a strong correlation between consistent Internet use and perceived skill and benefits, but there was also a strong positive correlation between Internet use, perceived skill, and risk.

Hypothesis 1A: Higher levels of social networking self-efficacy have a negative influence on perceived risk and lower levels of self-efficacy have a positive influence on perceived risk.

Social Networking Self-Efficacy and Trust:

Self-efficacy is usually related to the level of experience one has with a task. Social networking is not a particularly difficult task, but experience helps to judge whether a task is worth the risks or the benefits that may come from it. Another trait that experience influences is trust. The level of trust someone has in the credibility or safety of a website or Internet use is directly correlated to the level of experience one has with the Internet as a whole (Jones, 2009). In "Trust Influencers on the Web," a person's experience and web ability were assessed and compared with other factors to determine their levels of influence on trust. Although level of experience was only measured with one data point it was shown to have a positive correlation with the level of trust displayed for a website. The perceived ability was shown to have little effect on a person's willingness to trust a website. Since social networking has more to do with experience than personal ability it is believed that the level of experience for a site is directly correlated to a person's trust in a website.

Hypothesis 1B: A higher level of experience with social networking sites has a positive correlation with trust in social networking sites.

Perceived Privacy:

Social networking sites have changed the levels of privacy among friends and acquaintances. Further, the growth of social networking sites has increased the need for concern about information privacy. Social interaction in real life brings many different relations among people, however social networking sites, reduce relationships to simply being friends or not (Gross and Acquisti, 2005). Many people on social networking sites are willing to connect with anyone on the site, while others are more conservative. Since consumers can only categorize others as friends or not, some are more likely to accept people that they barely know or trust. Consequently, social networking sites present interesting privacy concerns for consumers. The risk for the unsuspecting or unaware consumer becomes great and the need for privacy protection for consumers becomes significant.

There are many different aspects the consumers of social networking sites will need to consider with regards to their need for privacy. For example, a consumer might want to keep their information available to a small circle of friends, but not with the general public. There are also cases where information can be made public but not to certain friends. Research studies have found that the consumers of social networking sites wish their personal contact information such as their email, phone, and instant messenger screen name to remain private. (Dwyer et. al 2007) Acknowledging this right to privacy and safety, most social networking sites have made it possible for consumers to keep this information secret. Still, these privacy concerns bring about the need for protection from the social networking sites themselves.

While the desire for privacy and safety among some consumers is important, some consumers seem to want to do little or do not actually know how to protect themselves. The consumers seem to want their privacy on social networking sites and also want their privacy and protection provided by the social networking site by default. In fact, researchers have found that many consumers care about their privacy, but they are less concerned about making sure their information stays private (Dwyer et. al 2007). This situation is very interesting because the degree to which a consumer on a social networking site is exposed is vast. There are thousands of consumers that are friends of a friend of someone. This allows the qualifications to be someone's friend on a social networking site to be very low (Gross et. al 2005). Further, increasing the circle of friends increases the risk and virtually decreases privacy. Thus, the need for privacy protection for consumers against other consumers increases greatly. Further, as the consumer's connections grow, the perceived privacy protection influences the consumer and their perceived risk.

Hypothesis 2: Perceived Privacy protection directly influences the consumer's perceived risk.

Perceived Security:

Consumers have inherent expectations on how secure any type of transaction should be online. The general expectation is that any intentionally undisclosed or withheld information should remain private. Additionally, it is typically assumed that any online identities such as user accounts will remain under the full control of the individual that created them. For example, a user logging into Facebook can reasonably expect that anyone without permission will not be able to control their profile. Similarly, any information that is placed online for a select group of

people or for one purpose should not be accessible to strangers or the general public. This premise has been supported by research conducted by The University of North Carolina at Chapel Hill (Pomerantz, 2006). In a study on the identity sharing behavior of students at the university, 38 undergraduate and graduate students were asked to identify what personal information they disclosed about themselves from a list of commonly shared information on social networking sites. Over 80 percent of users on social networking sites willingly disclosed information about their name, email address, friend network, gender, and academic classification. On the more extreme end, less than 20 percent of individuals willingly disclosed phone numbers and less than 65 percent of individuals disclosed any address information. Included in the survey were questions related to online privacy and security, a majority of respondents indicated that they were willing to let friends, family, classmates, and even strangers access social networking sites on their computers. This seems to indicate withholding of information is not simply a privacy concern, but a security concern as well. When respondents were asked whether they felt their identity information was safe online, the majority of respondents disagreed or was neutral. Furthermore, most respondents stated that they either agreed or strongly agreed that protecting their information was important to them. For these reasons, perceived security plays a significant factor into how risky consumers are when using social networking.

Hypothesis 3: How secure a social networking site is perceived will directly correlate with the perceived risk of disclosing information on the site.

Reputation:

Companies, organizations and interest groups have adopted the use of social networking not only for marketing purposes but also for reputation management. Similarly, public figures such as celebrities and politicians use social networking platforms in order to maintain and spread their particular self-images. As online social transactions become more commonplace, there are increasing expectations that individuals maintain a similar image online as they do in person. Workplace professionals are expected to maintain online presences that will not embarrass themselves and the organizations they work for. Many job screenings require an online background check of job candidates to ensure nothing incriminating or potentially damaging can be found.

Previous research has shown differences between levels of social networking use based on an individual's job or role in society (Landman, Matthew P. 2010). Matthew Landman and several other researchers studied the social networking habits of the resident and faculty population of Vanderbilt's department of surgery. The common assumption is that residents, while still highly educated and professional individuals are typically subject to less scrutiny than faculty who are expected to act as professors, mentors, and role models. Results of the study confirmed that social networking sites such as Facebook were used a lot less frequently by faculty in comparison to residents. While 64% of all residents surveyed had Facebook profiles, only 22% of faculty had profiles. However, a higher percentage of faculty with Facebook pages were more likely to have publicly viewable profiles. Of the 66 residents with Facebook profiles, only 25 had publicly viewable pages compared to 17 of the 28 faculty members. In general, individuals with an interest in maintaining a high degree of professionalism online tend to use social networking with less frequency.

Given the effect personal reputation has on social networking use, there is strong likelihood that the reputation of a social networking site itself also plays a significant role in information disclosure. (Patchin, J. and Hinduja, 2010) Researchers Justin Patchin and Sameer Hinduja published a paper under Sage journals in 2010 on adolescent use of MySpace over time. The team performed a content analysis of the profiles of 2423 adolescents on MySpace in 2006 and performed a similar follow-up analysis in 2007. The two concluded that even over this one year period, a noticeable decrease in numerous risky disclosure behaviors occurred. Additionally, a statistically significant number of users decreased their online activity or completely abandoned their profiles altogether. Given the negative publicity and reputation MySpace garnered over this period, as mentioned in the history of social networking, it is very plausible this influenced participant behavior. This idea is further supported in Kim's decision support model on consumer intention to use. The reputation of commerce websites was statically proven to impact levels of perceived trust.

Hypothesis 4A: Social networking sites with high reputation will have a higher level of consumer trust.

Hypothesis 4B: Social networking sites with high reputation will have a lower level of perceived risk.

Transference of Trust And Consumer Trust:

Whereas the reputation of the user has an impact on the perceived risk and perceived benefit of social networking, it does not have a noticeable impact on the trust the user places in a social networking site. Social viewpoints have been shown in several different studies to have an

impact in the trust one has in person or in a website. This influence from social viewpoint is best described as transference of trust.

Transference of trust is the high level idea that impressions made in the past influence present-day decision making. (Kim, et al., 2008) Kim discusses how trust can be transferred from members of a certain culture. Cultures are divided into two types, Type I and Type II. Type I cultures are individualist cultures where the opinion of the self trumps the opinion of the collective; whereas type II cultures are family oriented. Kim concluded that this difference in culture type indicated that transference based trust was much stronger in Type II cultures than in Type I cultures (Kim, et al., 2008).

Although the importance of culture on transference-based trust is not the focus of this paper, transference has been shown to have a great impact on the cognitive processes of the average consumer. Kim decomposed transference-based trust into two subcategories, referrals and third party seals. (Kim, et al., 2008) A referral is a recommendation by word of mouth, and the third party seal is an endorsement from a credible institution or company. Both of these concepts are reinforced by recent research on brick and click retailers.

A brick and click retailer is defined as a retailer who has both an offline store, as well as an online website to handle online purchases (Kuan-Yu, 2007). Different factors that influence the consumer's decision to purchase an item from a brick and click retailer's online website were investigated. Multiple conclusions were drawn, one of which was that offline referrals led to an increase in a consumer's trust of online purchases (Kuan-Yu, 2007). The trust in a website by friends and family outside of the Internet directly transferred to the consumer and led to a consumer's willingness to purchase. Further, the researcher revealed that offline trust is positively related to online trust (Kuan-Yu, 2007). While Kim's conclusions deal with referrals,

this conclusion strictly relates to trust decisions made in the past. The consumer interacts with the retailer in their physical store, and develops a level of trust in that retailer. This impression transfers over to the retailer's online presence. These two conclusions may directly apply to social networking. Instead of the consumer taking offline trust and applying it towards the online world of e-commerce, the consumer is applying that trust towards self-disclosure on a social networking website.

In "Trust Transference on the Web," Katherine Stewart introduces the term "entitativity." Entitativity refers to someone combining a group of individuals with similar attributes into a perceived collection. The initial person perceiving this group goes through a cognitive process where an impression is formed for one individual, and this impression is duplicated throughout the group, to reinforce the initial impression. This perceived group of people only needs one trusted individual, then that trust is transferred throughout the group. Entitativity is broadened from groups of people to similar items like websites. This is a powerful concept when applied to the social networking area due to the interconnectivity of the users. For example, through entitativity the user of a social network may clump all friends together as a tightly knit unit. Through the trust in one individual in this collective, the social network user may be more apt to trust the whole community (Stewart, 2002).

As described above, there are many methods of transference-based trust. Transference-based trust is an important topic that should be studied in order to understand why people choose to trust social networks and ultimately disclose personal information. During the consumer's cognitive processes, the consumer takes an initially neutral source and forms a new trust, for better or worse, partially based on these methods of transference-based trust.

Hypothesis 5: Transference-based trust will impact the consumer's overall decision to trust an online social networking site.

Consumer Disposition to Trust

Although some of the trust one feels is contributed by the trust others around him/her feel, the innate trust that one has plays an important role in the level of trust one places in any new source or situation. This innate feeling is often characterized by repeatedly trusting people or technology without a concrete or cognitive reason.

Disposition to trust is a personality trait that measures the degree to which users are willing to depend on others. In relation to social networking, disposition to trust may manifest itself in two ways, the disposition to trust in technology and the disposition to trust in people. Disposition to trust in technology or social networking likely inclines a consumer to use social networking for some purpose. As social networking is not complex in many technological ways, this most likely does not largely influence the decision to use a specific social networking site. The disposition to trust in people should have a larger influence on the consumer's trust of social networking sites. For example, disposition to trust in people may predispose someone to post more information about themselves online or use more group based services on these sites. Previous studies have demonstrated that higher levels of personal trust positively influence one's activity on a variety of electronic websites. Specifically, a study by Byoungsoo Kim and Ingoo Han of Korean university students affirmed their hypothesis that disposition to trust positively influences trust belief in relation to community-driven knowledge sites, a specific category of social networking sites (Kim, Byoungsoo 2009).

Hypothesis 6: A consumer's disposition to trust in people has a positive influence on willingness to trust social networking sites.

Consumer Personality Type and Intention to Disclose:

Disposition to trust is not the only personality factor being tested. Through research it has become clear that the personality type of the consumer is a determinant that must be considered when it comes to disclosing personal information through a social networking site, such as Facebook. Throughout the years, many different theories have been created to attempt to describe an individual's personality type, however the model that has been accepted by society is the Five Factor Model. This model contains five major categories that together describe a person's personality, hence the nickname the "Big Five" traits of personality. These categories are Neuroticism, Extroversion, Openness to Experience, Agreeableness, and Conscientiousness (Digman, 1997).

While sometimes the names of these categories differ from author to author, their meaning is the same. Neuroticism, the first of five personality traits, is sometimes referred to as emotional stability. A Neurotic person is emotionally unstable; their mood may be happy one moment and depressed another. The second personality trait of the Big Five model is Extroversion. The extrovert is someone who is outgoing; he or she is the center of attention in a group of people. Third is Intellect, also known as openness to experience. Someone who is open to experience is very willing to try new things. Next the model describes Agreeableness. An agreeable person is someone who is amiable; an agreeable person avoids hostility by sometimes agreeing about something they do not necessarily believe. Finally, the last trait of the Big Five

model is Conscientiousness. A Conscientious person is diligent and organized with day-to-day life (Digman, 1997).

Research has been conducted applying the Five Factor Model to the topic of social networking. Out of the "Big Five" categories, only Neuroticism and Extroversion were found to have a measureable impact on Facebook use. Extraverts were found to belong to many more groups on Facebook. Since the extravert is outgoing with people offline, they will be outgoing online in a social networking environment (Ross, 2009). Subjects high in neuroticism were found to use the wall component of Facebook the most. This is believed to be because text can be as revealing as you choose it to be, and it can be edited or deleted. A neurotic person can spend as much or as little time as they please controlling what is posted. On the other hand, neurotic types do not post pictures very often. A picture can inadvertently reveal information that a neurotic personality type may not want to reveal, such as location, or emotional states. While hypotheses were made regarding the other three personality types, no conclusive evidence was found to create a strong link between Openness to Experience, Agreeableness, and Conscientiousness to Facebook use. (Ross, 2009)

Additional research related to personality types and social networking has become popular over the last couple of years. From a general consensus of the authorities in this area, the Extrovert personality factor has the most significant impact on social networking use. Extroverted users tend to use social networking websites frequently. The belief behind this statement is that extroverts have already used their skills to create an offline network of friends, but desire an even larger one. Extroverts want to boost their image, so they do this through online social networking. (Correa, 2009)

Additional research supports these results. It was found that extroverts tend to have more friends on Facebook than their introverted counterparts. An introvert is the opposite of an extrovert. The introvert is a reserved person, who would rather listen to a conversation than be at the center of it. The median amount of friends an extrovert had on Facebook was found to be 150, versus the introvert, which was found to be 103 friends. An interesting note from this research was how the different personality types acted on Facebook. It was found that extroverts may have had more friends on Facebook, but they did not have as much information on their profile compared to introverts. (Amichai-Hamburger, 2010).

Zywica introduces two hypotheses that further elaborate on extroverts and introverts using social networking websites. The first of these hypotheses is the Social Compensation hypothesis. The Social Compensation hypothesis applies to introverted type personalities. The concept is that introverts tend to compensate for their lack of offline social skills by being active social networking site users. Introverts throw away their undesirable offline contacts and instead replace that hole with a network of online friends. In order to compensate for the lack of self-image they have offline, they tend to include much more information on their profile than an extrovert would, and also go above and beyond by exaggerating. An introvert is much more likely to disclose personal information which may be viewed as risky than an extrovert because an introvert tries to create a desirable online personality (Zywica, 2008).

According to the Social Enhancement hypothesis, extroverts, like introverts also use social networking sites, but they have a different purpose in mind. An extrovert's skill set comes into play in real life, when in close proximity to other people. Extroverts use Facebook to preserve the image that they have created offline. In return, the typical extrovert tends to be

boastful in an attempt to gain more friends to add on to their current network of contacts (Zywica, 2008).

Researchers have dedicated many hours to try and understand how personality affects social network use. By reviewing the research conducted on this area, it is most practical to narrow the Five Factor Model, and focus on the Extrovert personality factor. The majority of research conducted link extroverts to social networking site use. In our study, our main goal is to understand what leads to self-disclosure on social networking sites, so it is most appropriate to focus on the self-disclosure of extroverts and introverts since this is where most of the research in this area points. However, the other four personality traits of the Five Factor Model will be tested as well. Overall research has revealed that personality type is a big factor in a consumer's intention to disclosure personal information on social networking websites; therefore it is crucial to include this concept in our research model.

Hypthesis 7: Personality type plays role in how much benefit is derived from social networking sites.

Hypothesis 8: Personality type plays a role in a consumer's intention to disclose personal information on a social networking site.

Perceived Benefit:

Several theories have been proposed on what comprises perceived value of a social networking site and how much this value ultimately influences use and disclosure on a social network (His-Peng, 2009). One previous theory analyzed the influence of extroversion and introversion on intention to pay for social networking sites. Among factors that influenced perceived value were the emotional value, social value, value relative to price, and quality value.

An online survey with 223 respondents was used in order to test the theory that these four values would influence aggregate consumer perceived value of a social networking platform. Results indicated that emotional value, social value, price value, and quality value were all statistically significant in having an impact on perceived value. Additionally, it was determined that these factors were directly influenced by the personality type of the consumer. Figure 4 shows the statistical results of this study. Self-proclaimed introverts among respondents demonstrated higher weighting of the emotional values of social networking while extroverts among the respondents demonstrated a higher weighting of social values. Introverts furthermore placed more weight in the performance and quality value of social networking sites than extroverts while price value did not seem to differ between either of those two groups.

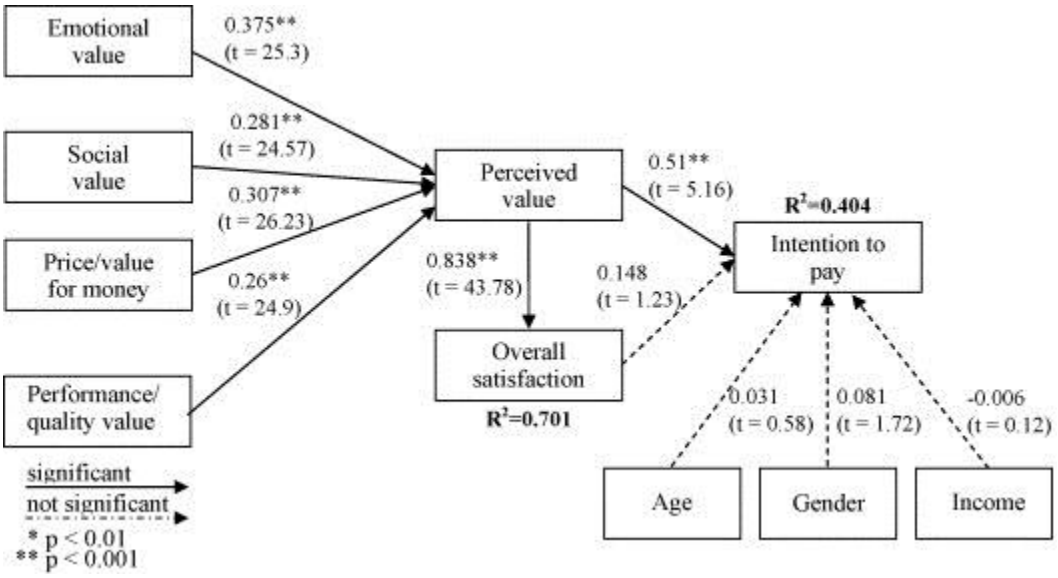


Figure 4: The final results linking the underlying factors of social networking to perceived value of the site from "The influence of extro/introversion on the intention to pay for social networking sites" by His-Peng et al.

Research published in May of 2011 examined why people used social networking sites from a motivational theory approach (Kuan-Yu, 2011). Among their hypotheses was that perceived benefit is derived from the combination of usefulness and enjoyment. In this case, the

usefulness of a given social networking site was based on whether it could enhance a person's work or job performance. Enjoyment was based on how much pleasure a given consumer received from the use of a given social networking site and was largely left as an intrinsic factor. Moreover, both these components of perceived value had a direct relation to continued intention to use a social networking site. Results of the study, which involved 402 online respondents, concluded that perceived usefulness and perceived enjoyment both had statistically significant effects on the continued use of a social networking platform. However, perceived enjoyment more greatly influenced a user's decision to use social networking with usefulness as a second priority. Network externalities such as number of members, number of peers, and perceived complements all had statistically significant influences on usefulness and enjoyment. However, the number of peers and members on a social networking site had significantly greater effect on perceived usefulness of a website than perceived enjoyment. Enjoyment is not as significantly affected by the large number of users of a platform which may indicate enjoyment is based more on emotional, social, or quality values.

Hypothesis 9: Enjoyment derived from emotional and social value has the strongest influence on intention to use and disclose information on social networking sites.

Consumer Trust and Intention to Disclose:

Social network disclosure is moderated by the trust of each of its members. Trust is a very important factor for social networking sites. It is the consumer's trust that determines his or her willingness to share personal information (Dwyer, 2007). Trust in the people they interact with affects the consumer's intention to disclose personal information on a social networking

site, and it also affects the consumer's use of the technology on the site. Since social networking sites service millions of people and are often open to everybody, consumers cannot trust everyone and rely on the privacy policies within the sites to protect them (Dwyer, 2007). Many times the consumer is hesitant to disclose information about themselves when there is an inadequate level of trust in the privacy policies of the site.

When the consumer has enough trust to link their profile with another, they are showing that they trust the person they are linking with and the privacy policies of the site. The act of linking profiles is saying that the consumer trusts the person enough to disclose their information. Thus a consumer's intention to disclose information on a social networking site is directly affected by their perceived trust with other consumers. This trust in other users of the social networking site can be shown if the consumer is willing to meet new people (Dwyer, 2007). Consumers are more willing to disclose information in the pursuit of meeting people, so the sense of trust a consumer has in order to meet people affects their intention to disclose information.

The consumer's intention to disclose information is also affected by their trust in technology. The consumer relies on the social networking site to not divulge their information and to keep it private (Dwyer, 2007). If a consumer has relativity high trust that their information is not being misused, then their intention to disclose will be higher. On the contrary, if a consumer does not trust that their information will be used properly, their intention to disclose information will be a lot lower. The level of safety and privacy that a social networking website offers the consumer to protect their information helps to gain their trust and increase their intention to disclose personal information on the site.

Hypothesis 10: A consumer's trust in the technology and people behind a social networking site directly affects their intention to disclose information.

Perceived Risk:

The privacy and protection of consumer information is not the only security concern consumers have about disclosing information. A major contributing factor to a consumer's perceived risk on a social networking site is the growing number of targeted phishing and malware attacks. These cyber-attacks are a deterrent on a consumer's willingness to trust a social networking site. This distrust increases their perceived risk of a site and often deters their intentions to disclose information (Kenyon, 2010).The threat that cyber criminals present should have a direct outcome in a consumer's perceived risk.

Usually, sites that can act as a front to these malware attacks are often legitimate sites that have been hacked by cyber criminals (Antony, 2006).A consumer's perceived risk is based off the trust that a company will protect their site from attacks and in return protect the consumer from attacks. Companies that wish to maintain a creditable site need to take measures in protecting their consumers. The consumer's perceived risk has been found to influence the online decisions taken by the consumer (Antony, 2006). There is a link between perceived risk and intention to disclose information on social networking sites. Thus, the perceived risk has a negative impact on consumer's intention to disclose information (Kim, 2008).The more a consumer's perceived risk goes up, the less likely the intention of the consumer will be to disclose their information.

A consumer's perceived risk can affect their intention to disclose his or her personal information on a social networking site. For example, if a consumer believes the risk is too great,

he or she will not disclose as much information as another consumer who sees the risk as minimal. In fact it was found that only about 10% of consumers on Facebook posted his or her phone numbers and home addresses (Fogel, 2009). This can show that the perceived risk on disclosing this information is too much for most consumers. The amount of risk the consumer perceives with a social networking site affects their intention to disclose information.

Past research has indicated that how risky a particular social networking site is perceived factors into consumer decision to adopt and frequently use it (Fogel, 2009). In 2008, 205 students at a four-year university were given an anonymous study including questions regarding trust, privacy, and risk taking on social networking sites. Questions were largely in reference to the social networking sites Facebook and MySpace and other social networking sites were referenced as "another social networking site". Results showed that men were more prone to risk taking behavior while women more often had greater concern for what they posted on the Internet. Men were approximately 9% more likely to include a picture of themselves than women (90.4% to 81.6%), were over three as likely to include a phone number on an online profile (14.5% to 3.9%) and were nearly twice as likely to include home address information on an online profile (12.0% to 6.6%). Despite greater risk aversion, women tended to browse more online profiles daily, browse profiles longer, were more likely to personalize their profile pages, and were significantly more likely to write on other people's pages. Both men and women had higher perceived trust for Facebook versus MySpace which also correlated with higher adoption. 76.8% of respondents indicated that they created an online profile on Facebook at some point in time while 51.6% of respondents stated they once created an online profile on MySpace. Only 32.7% of respondents said that they had ever created an online profile on another social networking site (Fogel, 2009).

A study conducted in 2009 by researchers from the Handboldt University of Berlin developed a model for social network self-disclosure that considered perceived risk as the product of two variables, perceived likelihood and perceived damage (Krasnova, 2009). Perceived likelihood is the subjective probability that a negative event would result from self-disclosure. Perceived damage is the subjective assessment of the impact a negative event resulting from self-disclosure would have. The results of the study revealed statistically significant correlation between levels of self-disclosure and perceived damage and likelihood of damage. However, perceived likelihood represented a significantly higher concern among respondents than any perceived damage.

Hypothesis 11. Perceived risk is influenced largely by perceived likelihood of negative consequences or level of trust.

Hypothesis 12. A consumer's perceived risk negatively affects a consumer's trust in a social networking site.

In order to test the following hypotheses and constructs, a sufficiently large amount of data on consumers in relation to these constructs was needed. Our team determined the most appropriate manner of collecting such information would involve creation and distribution of a survey with questions based on these constructs. The entire model's validity could be determined by the relation between the average responses from multiple question types. Questions would be taken or reworded on the various literature and research supporting our theoretical disclosure model.

Methodology:

Previous studies have sought to determine the Measurement Equivalence of surveys conducted using pencil and paper and surveys conducted through computer or web-based means (Reynolds, 2011). Measurement equivalence is a term used to describe the stability of a measure's structure across situations, such as measures that are performed using pencil and paper or when using electronic or other means. Current research indicates that most measures perform equivalently regardless of medium with the notable exceptions of speed tests and measures of beliefs and affect towards computers. While a speed test can be avoided, the difference in equivalence regarding perceptions of computers may affect the quality of data if both electronic and pencil and paper surveys are used.

Reponses rates to online surveys are typically considered acceptable if they are around 50%. Higher response rates around 60% and 70% are considered good and very good (Kaplowitz, 2004). Previous studies have resulted in conclusions on average email response ranging from 24% to 76%. These same studies indicated an average response rate for web-based surveys around approximately 30%. More recent studies indicate that this gap in response may not be as wide as previously thought. Research in 2008 concluded that web based surveys on average have response rates 11% lower than alternatives. More specifically, response rates were 12% lower than mail based surveys, 13% lower than email based surveys, and 13% lower than phone surveys. Web-based surveys are also more susceptible to non-response bias. Using multiple modes in conducting surveys has been shown to moderately improve response rates. However, respondents to aural or ear based surveys such as telephone interviews tend to have more responses on extreme ends in comparison to visual surveys. For example, a survey respondent is more likely to give a higher product or company rating during a telephone

interview than they would on a visual survey conducted through the Web, Internet, or Mail. According to research, which analyzed surface mail versus web mail, the most efficient way to get survey response rates was to send physical hardcopies of the survey to the target audience. However, when a physical notice was distributed before a web survey as a pre-notice, a web survey was found almost as efficient (Kaplowitz, 2004). Given the ease of conducting a web based survey in a limited resource environment and the availability of university tools for targeting large numbers of potential respondents, our IQP group decided to conduct our survey online.

Our intention was to implement a web-based survey using the best practices determined by previous academic studies. Major factors that affect response rates for web surveys include content and presentation. Without adequate feedback on the content and presentation of a web survey, there is little way to determine how respondents will perceive it. Multiple revisions of the survey were performed along with pilot testing in order to correct all manner of issues that may have inhibited response. Ease of accessibility determines how likely it is individuals will respond to a survey. If extensive effort is necessary in order to even access the location of a survey, there is high probability of non-response. Addressing the manner of web survey delivery was a principle concern which led us to use SurveyMonkey to conduct our survey. SurveyMonkey is an online survey software tool that allows for creation of both simple and complex surveys. Using professor Loiacono's premium membership, we were able to host the survey on the website without running into issues related to data integrity, accessibility, or data limitations. The survey interface is familiar and easy to use while offering plenty of utilities for collecting, distributing, and analyzing multiple academic surveys. Our IQP team also looked into understanding the level of computer use and understanding of the target demographic audience

in designing our survey. Fortunately, the technical background of our target respondents allowed for only slight alteration given a similar background of the project team.

Before conducting any sort of preliminary survey, it was necessary to first understand the demographics of the targeted group. The target group for our survey was the community of Worcester Polytechnic Institute (WPI). WPI's community is a diverse group of individuals. People from different genders, ages, and geographic locations comprise this community. According to the most recently published WPI fact book, there are 3416 undergraduate students on campus. 1032 of these students are female and 2384 are male. While a little over 71% of these students are Caucasian, WPI has a significant amount of other ethnicities. There are 159 Hispanic, 77 Black, and 145 Asian students on campus just in the undergraduate body. These ethnicities come from a number or different places around the world. 45 of the 50 United States are represented, as well as 62 other countries. These figures are just a brief synopsis of the diversity within WPI's community.

The real question at hand is how do the demographics of WPI relate to the demographics of social network users? Social networking is a worldwide phenomenon. There are 741,426,860 confirmed Facebook users as of September 25th, 2011. 155,745,780 of these near 800 million users are from the United States of America. Interesting enough, the age distribution of Facebook users is very distributed. Figure 5 below summarizes United States Facebook users.

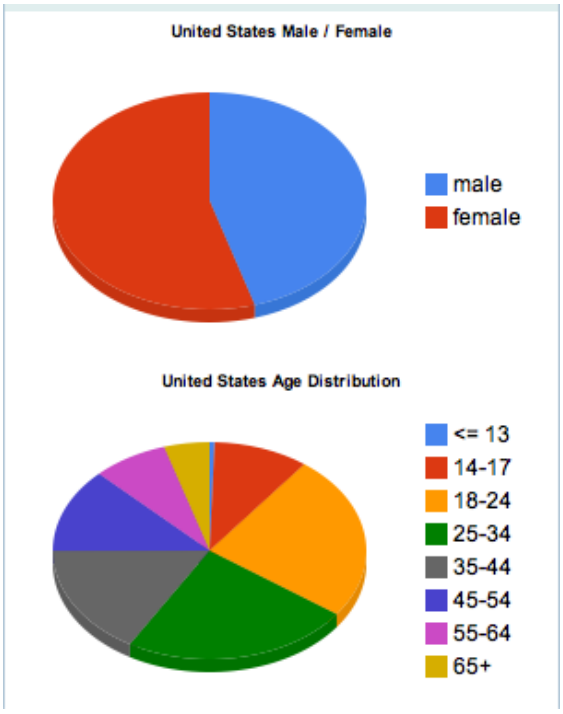
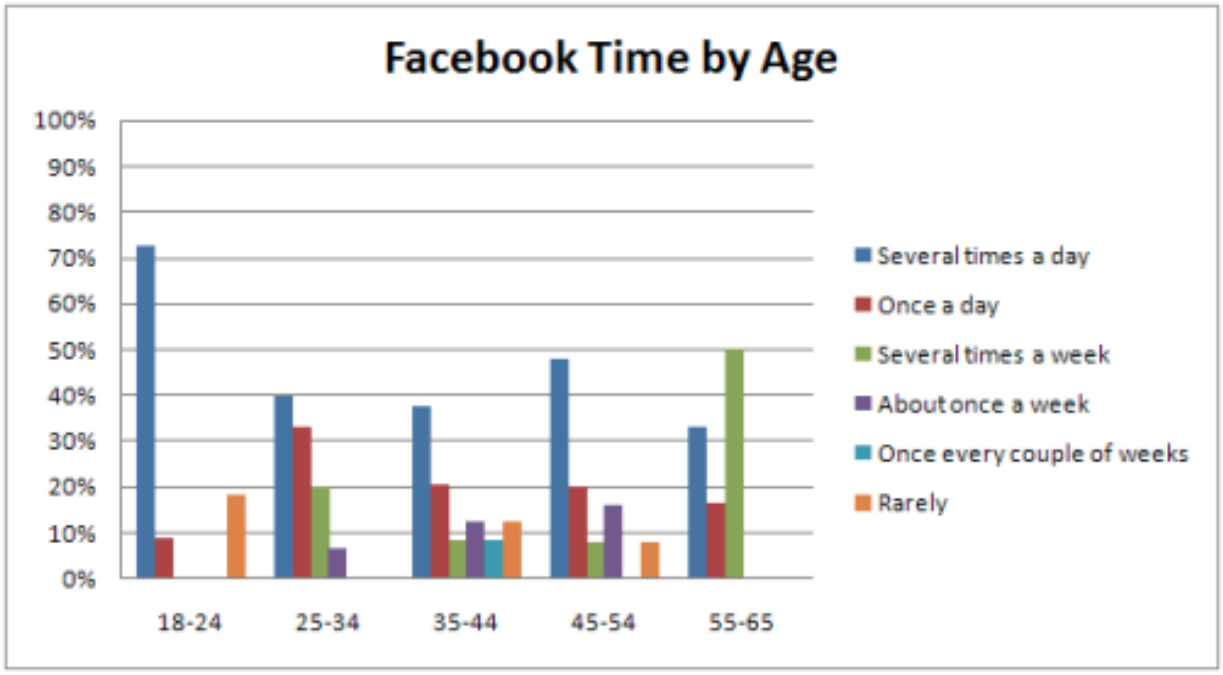


Figure 5: A pie chart representing the percent of users by age of Faceboo (Gonzalez, 2011)

The college age group of 18-24 years makes up about 25% of the pie chart pictured above. The 25-34 and 35-44 year age groups make up about 40% together. (Gonzalez, 2011)



While the number of users outside of our target group is significant, the big difference between the age groups is the amount of time spent on the website each day. Refer to Figure 6 below to see the average amount of Facebook use across age groups.

Figure 6: The time spent on Facebook by age groups (Crepeau, 2009)

The figure above supports our target group at WPI. As you can see, from the college age group of 18-24 years, the survey found that over 70% of the Facebook users visited the website several times a day (Crepeau, 2009). While the older age groups still visit the website, the rate is well below our targeted age group.

As described above, the majority of use comes from the average day-to-day college student. However, it is also important to consider social network users outside of this generic stereotype. To solve this problem, the survey will also be given to WPI faculty and staff

members. With the survey being delivered to this portion of WPI's community, we will successfully address a broad spectrum of social network users.

In a college setting, it is expected to regularly use e-mail. E-mail is provided free to the members of the WPI community, and it is used to communicate between community members. Delivering a physical survey to the target audience may return the biggest rate of responses, however it is infeasible. The cost of printing the surveys is excessive, and the topic of the survey would be better served through a web survey.

In order to improve the survey, it was given to several professors at Worcester Polytechnic Institute. Dr. E. Loiacono's help was instrumental in determining the best questions and format for the final survey. The survey was also delivered to several other professors with experience in this field of research to get a broad range of comments and suggested improvements. A consent form was also given to the participant according to IRB regulations. Appendix A has the script used for this survey.

On December 7th, 2011, the social networking survey was sent out to WPI students under the general student alias. This list contains approximately 4000 students ranging from freshmen to seniors. Students were given an incentive in the form of a chance to win a $100 VISA gift card to encourage a higher response threshold. Approximately 600 students responded by initiating completion of the survey. This represents an approximate 15% response rate from the email alias. Given the indirect means of contacting survey responses and large response total, this response rate was deemed a sufficient sample of the population. However, a significant number of respondents did not fully complete the survey. All users who did not fully complete all questions were marked for removal in the full analysis of collected data. Additionally, a number of survey respondents were flagged for various actions that jeopardized the integrity of the

survey. Inappropriate, underage, or clearly randomized responses were also removed. All survey data was stored in a Microsoft Excel file with sheets for each iteration of filtering. Each question received a header indicating what construct it was associated with and a number indicating what question number it was for that construct. The average values of each construct question were taken in order to analyze the construct as a whole. In some cases, such as with questions regarding consumer personality type, questions needed to be reverse coded. For example, responses for a question such as “I do not have a good imagination” needed to be reversed so that a 1 corresponded to a 7, a 2 to a 6, and so on. This was to ensure the consistency in question types where normal questions were worded such as “I use difficult words.” All survey data was normalized in order to ensure proper analysis could occur in SPSS, the statically tool used by our team. The final sheet of data simply contained question headings followed by raw data to ensure lack of errors during analysis.

Results:

Redacted on the request of Professor Eleanor Loiacono. For the full report, contact her at etl@wpi.edu

Discussion

Redacted on the request of Professor Eleanor Loiacono. For the full report, contact her at etl@wpi.edu.

Conclusion:

Redacted on the request of Professor Eleanor Loiacono. For the full report, contact her at etl@wpi.edu.

Research Implications and Limitations:

Several constructs were included in the survey that were not incorporated into the model. The constructs of Social Norms, Familiarity with Social Networking, and Attitude towards Using the System were not evaluated in regard to intent to disclose information on social networking sites. While these constructs were excluded in preference of testing constructs within the Kim (2008) electronic commerce model, it is probable that they do play a significant role in disclosure habits of social networking users. Due to the limited statistical knowledge of the group and the time limits of the project, only the core constructs were analyzed. It is recommended that further research on social networking disclosure include hypothesis linking these constructs to an overarching decision support framework. Unused survey data may be useful for expanding upon the model that was analyzed over the course of this project.

Certain background information collected could also be used in further research. Gender information, age, primary social networking site information, and online name use could be used to test theories related to disclosure habits of particular categories of individuals. However, limitations do exist on the amount of credible information that can be extracted from collected data. Most survey respondents fell between the age ranges of 18-22. Although this age group has the highest level of social networking use, any theories on social networking use verified may be limited to this specific age range. It would be interesting to expand the study to consumers of all ages.

Lessons Learned:

During the first seven weeks of project work, our research group encountered several problems in relation to research. Due to lack of experience or understand of decision support systems or empirical research models, initial work and assumptions were largely based on a few

key scientific studies and articles. In order to create a model that best reflected self-disclosure using social networks, the group had to branch beyond these select articles and include the findings from additional literature. Our model went through several revisions during this period in order to better capture the suggestions of advisors and a deeper breadth of literature. In several cases, we needed to break apart variables and create additional hypotheses in order to expand upon the models of previous researchers.

Work during the second term of the project was primarily based around creating a web survey that would appropriately match the model we were looking to test. Questions were based on previous research found in our literature review although slight modifications were needed. For example, questions regarding perceived risk were taken from research regarding perceived risk in using a social networking site. Our survey questions assumed respondents were answering questions about a specific social networking site they used which resulted in all questions being based on intention to disclose rather than intention to use. Question rewording was not always ideal and additional review could have been conducted before the release of the survey to the student body. Additionally, additional research looking specifically at intention to disclose rather than intention to use could have been sought out instead of rewording questions.

Response rate for the survey was about 15% and it should be noted that the financial incentive, a chance of winning a cash prize or gift card, was a sufficient way to achieve survey responses in the several hundred. One noticeable challenge was the difficulty in getting all participants to fully complete all 128 questions of the social networking survey. Approximately 200 respondents quit the survey early. Although we specified that the survey would take approximately 15 minutes to complete at the instructions, the sheer number of questions may have deterred respondents who did not believe this time limit would be sufficient. Prior test

groups proved this time was more than sufficient but having fewer questions may have had a significant impact on completion rate. Several groups of survey questions did not match to any constructs that made up the self-disclosure model. Question construct groups such as social norms, social networking familiarity, etc. had no direct connection to the developed model and could therefore not be used in the statistical analysis. This data may be usable in future research but it may have been more advisable to remove these questions from the survey in order to reduce the question total.

Future Research:

A majority of social networking site use is from high school and college students. Although the survey is largely focused on college aged consumers, it could be expanded to include high school consumers. We are looking into the possibility of expanding the survey to local area high schools to ensure that another major sector of social network consumers is covered. Our research is going to go towards building an interactive website or source of media to teach consumers about the implications of divulging information on social networking sites and better inform consumers of how to safely approach information on social networking sites.

Website Introduction:

While the main focus of our project was proprietary research related to the disclosure of information on social networking sites, we also needed to satisfy the demands of an Interactive Qualifying Project (IQP) at WPI. An IQP studies some form of interaction between society and technology, and then typically concludes with a deliverable which gives back to the community. In order to satisfy this demand, we decided create a tool which could be used to inform the public about the dangers of putting personal information on social networking sites. We sought

the help of a local information security professional, Mr. Neil Spellman in developing such a tool. Neil Spellman is a network analyst for WPI's network operations; he has dedicated most of his professional life to information security. Mr. Spellman frequently holds workshops which deal with information security and would benefit greatly from a tool he could use during his workshops.

Through multiple meetings with Mr. Spellman, it was decided that we could give back to the community by creating an interactive website which would be integrated into his workshops, and also with freshmen programs at WPI. Each new student at WPI undergoes a program called New Student Orientation during their first week of residency. During New Student Orientation, and also the first semester at WPI, there are multiple programs the students attend with their freshman floor, Resident Advisor, and Community Advisor. The topics of these programs are usually related to alcohol safety, available academic tools, etc. Starting next year, we hope to add a program which informs the new freshmen students about the information they disclose on social networking sites. The focus of this program will be our interactive website, which will inform the student about disclosing information on social networking sites, and start a discussion for the program.

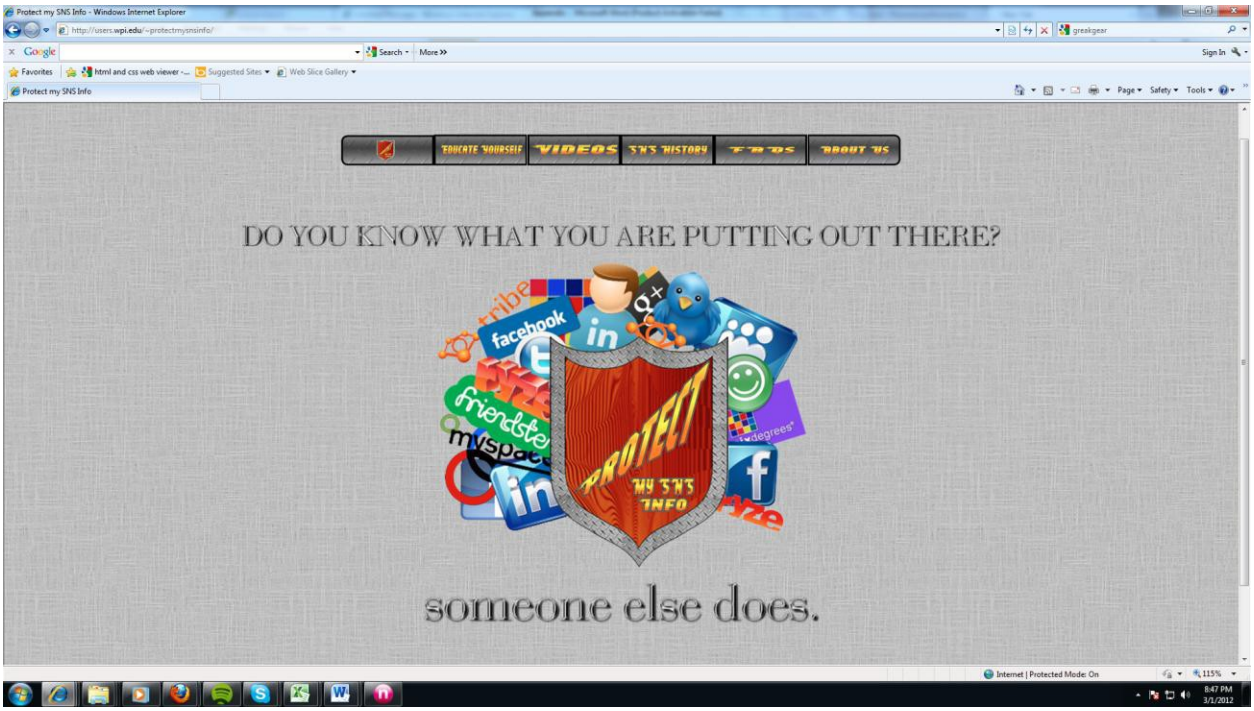
The Creation

Originally, the website would have information on Facebook, LinkedIn, Twitter, and Google +. This information would cover tutorials, quizzes and other educational materials. After talking to Niel Spellman, our team was advised to cut this content in favor of a more full-fledged section on Facebook. The purpose of the website was altered from a general help site to a resource specifically designed to help freshmen WPI students. In order to incorporate the website's educational tools into a freshmen RA program, the focus needed to be narrowed down.

Due to the popularity of Facebook over other social networking sites, this narrower focus was deemed more efficient for the purposes of WPI.

Our website consists of several main pages covering various topics and containing numerous links and images. The primary pages of the website include a home page, educate yourself page, Facebook test page, a videos page, a SNS history page, a FAQs page, and a about us section. The following pages are described in further detail in the following sections.

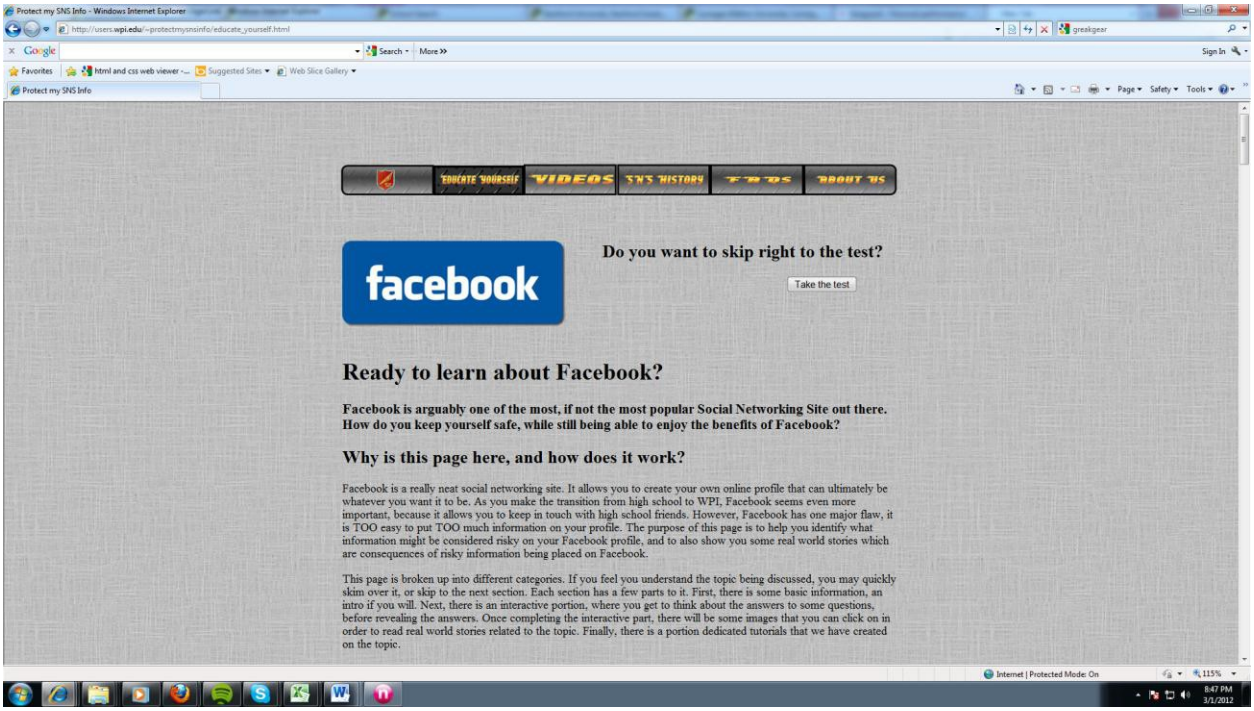
Home Page



The home page of our website is a clean page, bearing our main logo. Our main logo is the Protect My SNS Info Shield, with a variety of social networking sites behind the shield. Above our logo are the words “Do you know what you are putting out there?” and “someone else

does.” This short sentence conveys the point of the website in a nutshell. The purpose of our website is twofold, the first is to inform the public about the impact their information could have on a social networking site, and second to help the user learn how to stay safe while using social networking sites.

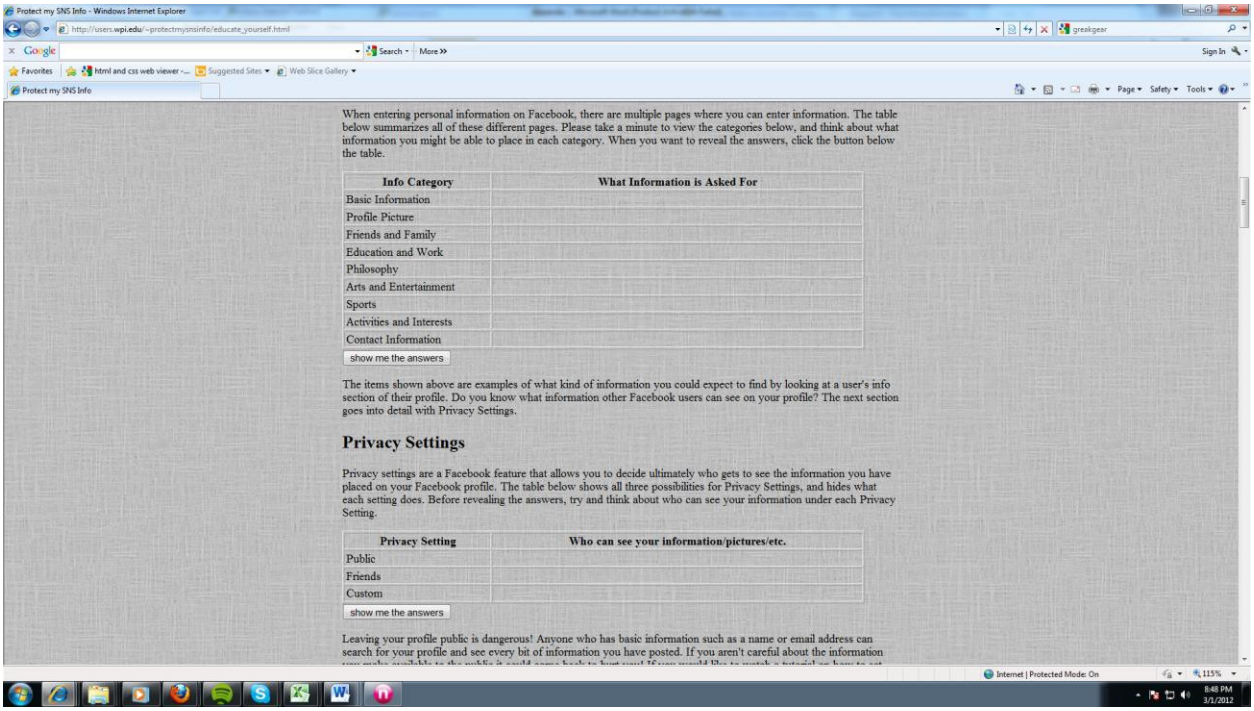
Educate Yourself



This page is the meat and potatoes of our website. The educate yourself tab contains all of our educational material which is used to educate the reader about Facebook. Originally, the website was planned to be broad, and able to cover multiple social networking sites. However, after speaking with Neil, we decided it would be best to narrow the scope of the website to just Facebook. The website will be used as a tool to help protect incoming Freshman WPI students on social networking sites. However, when looking at media, Facebook always seems to be the

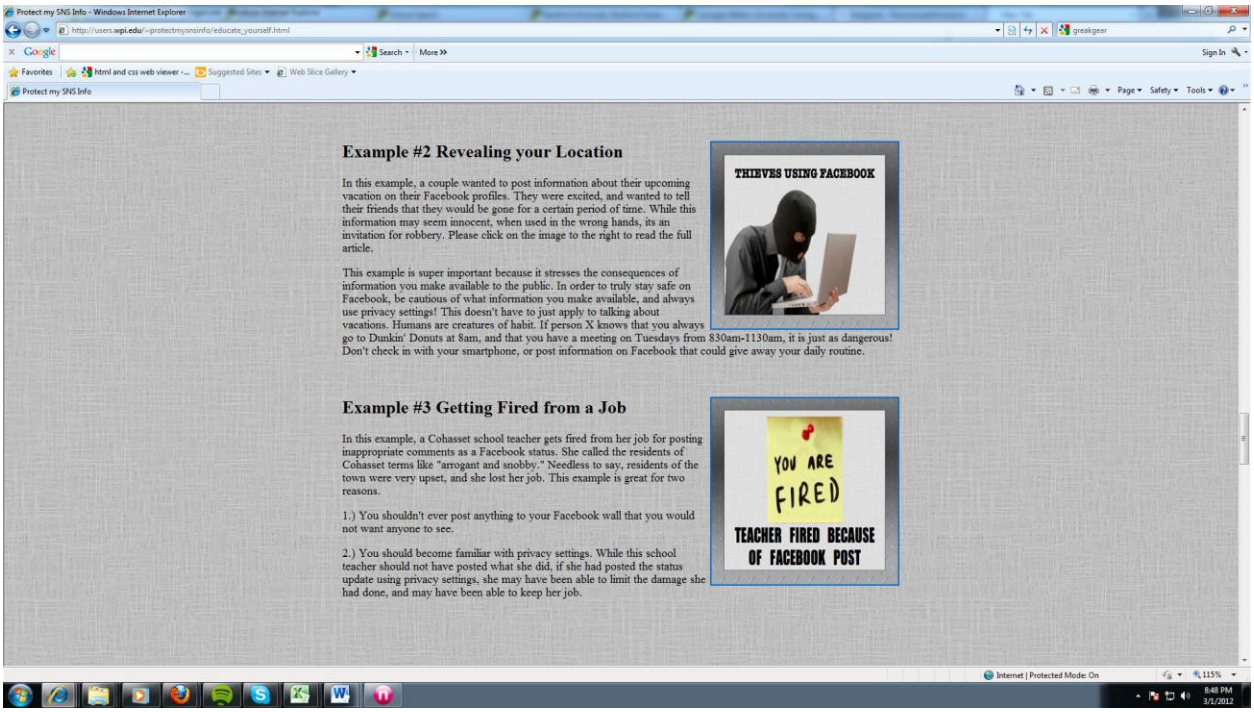
problem. Other sites like Linked In would be great to discuss, but it does not really apply to our demographic. The typical incoming Freshman does not have a professional profile on a site like Linked In.

After the basic description and introduction to the educate yourself tab, we get into talking about available information. Available information describes what information you can enter into Facebook fields. The material is presented through a table with hidden descriptions. The hidden descriptions allow the user to think about what material might be hidden before hitting the button below the chart. Clicking the button reveals the answers.



Next we begin to talk about privacy settings. Another table with hidden descriptions is introduced to help the visitor understand what the three privacy settings on Facebook are. To reinforce the importance of privacy settings, our first tutorial is supplied. In the first tutorial, We introduce two silly characters, Sno W White, and Da Wolfe. In the tutorial, we show the visitor how to use privacy settings when uploading pictures, through the characters.

Now that we have covered what information might be present on a Facebook profile, and also how to hide that information, it would be desirable to discuss what information might be potentially risky on a Facebook page. We have another table in this section, which splits a few example bits of information into good and bad columns. Once the visitor reveals the answers, he or she may go on to read an article we have provided. The article discusses how a stalker may use Facebook with malicious intent. The second tutorial deals with how to block other Facebook users. Say for example you find out someone is trying to stalk you through Facebook, it would be important to know how to block that profile.

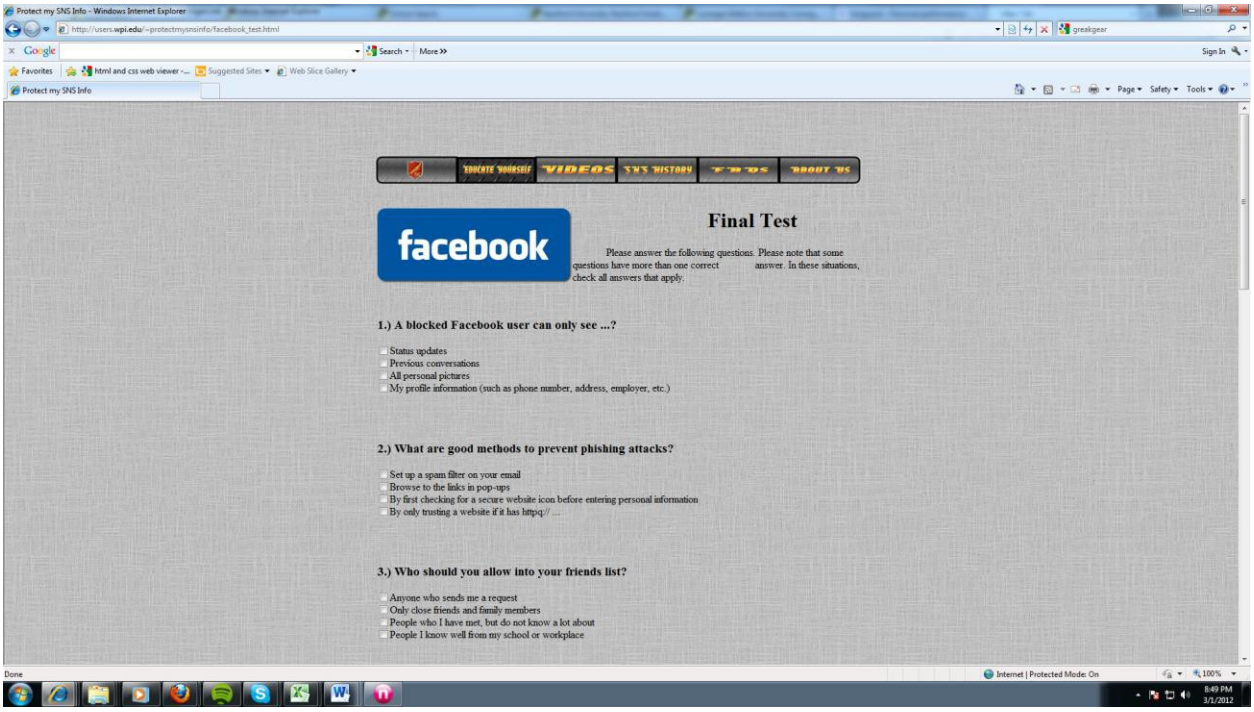


After discussing risky information, we dive head first into status updates. Risky information does not have to be static on Facebook, but can be more dynamic as more and more information piles up through status updates. After a brief introduction to status updates, we provide another interactive table to get the visitor thinking about wall posts. This table is succeeded by three links to articles. The first link goes into detail about what the consequences

are of posting vacation time on Facebook. The second describes a story of how a schoolteacher was fired after complaining about her students on Facebook. The final article links to a paper on how human resources are beginning to filter out prospective job candidates based off of Facebook profile information. These articles are followed by a third tutorial. This tutorial discusses status updates, and how to narrow who can see status updates.

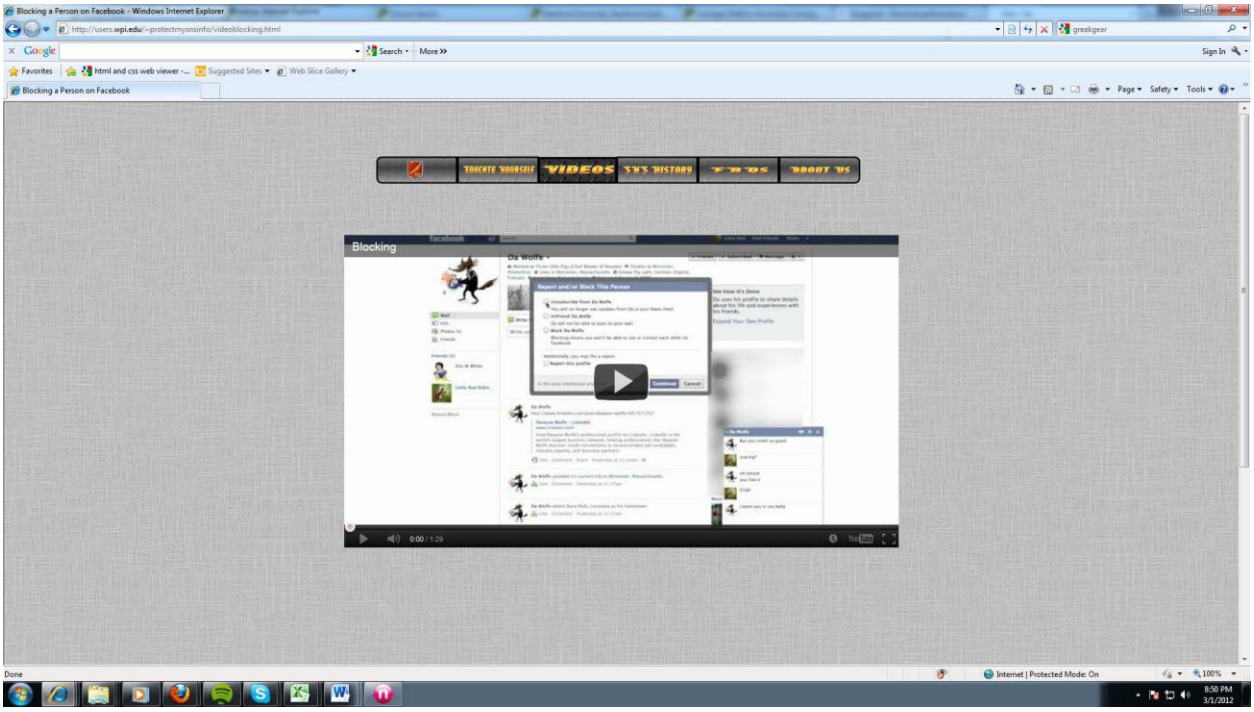
Finally, we conclude the educate yourself tab with phishing. We introduce the visitor to the concept of phishing, and provide a few tips with how to avoid becoming a victim of phishing. This introduction is followed by two life examples of phishing. The first link brings the visitor to a chase website, which speaks on email phishing. The next link brings the visitor to a Blizzard games website which discusses in-game phishing. Once finishing our education, you may browse to the test page.

Facebook Test



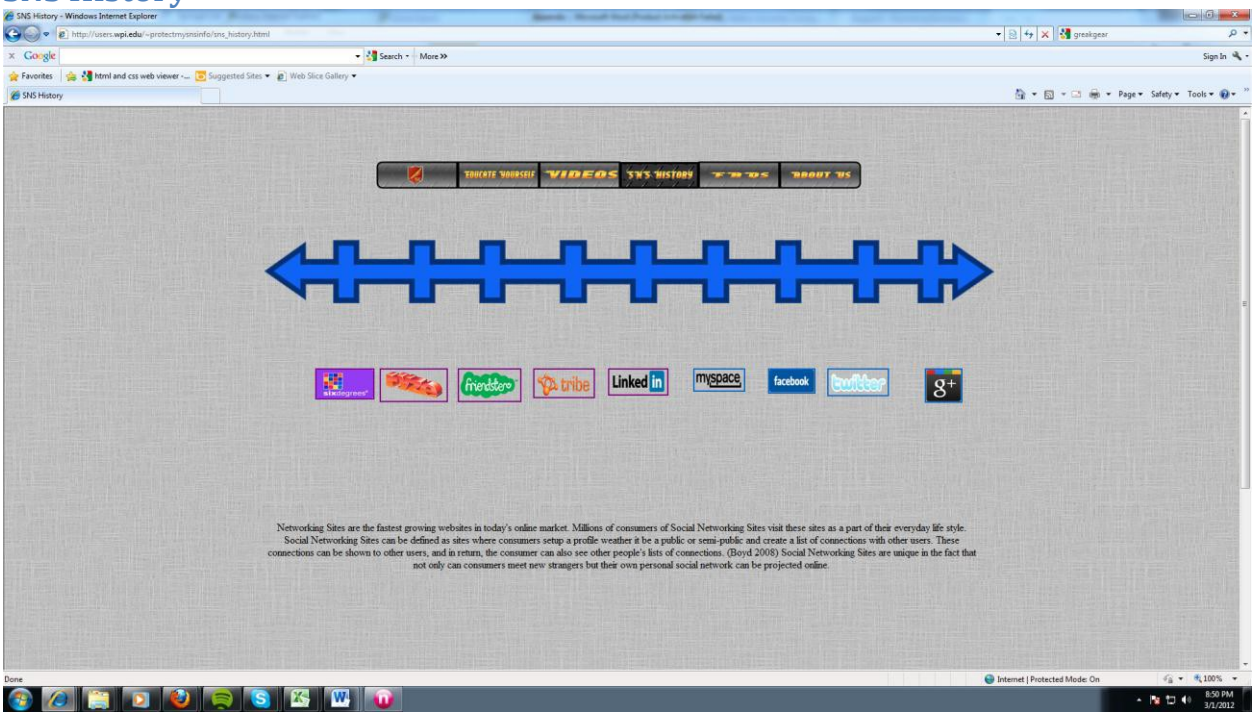
On the Facebook test page, there are ten questions in total. Each of these questions reflect an important concept that should have been learned through reading the educate yourself page. When finishing the test, you can press the submit button and see your score. If the visitor is not pleased with their score, they have the option to reload the page and take the test again, or reveal the answer. If the visitor reveals the answers to the test, then the correct answers are highlighted in green, and a description of the why the answers are correct is displayed under each question.

Videos



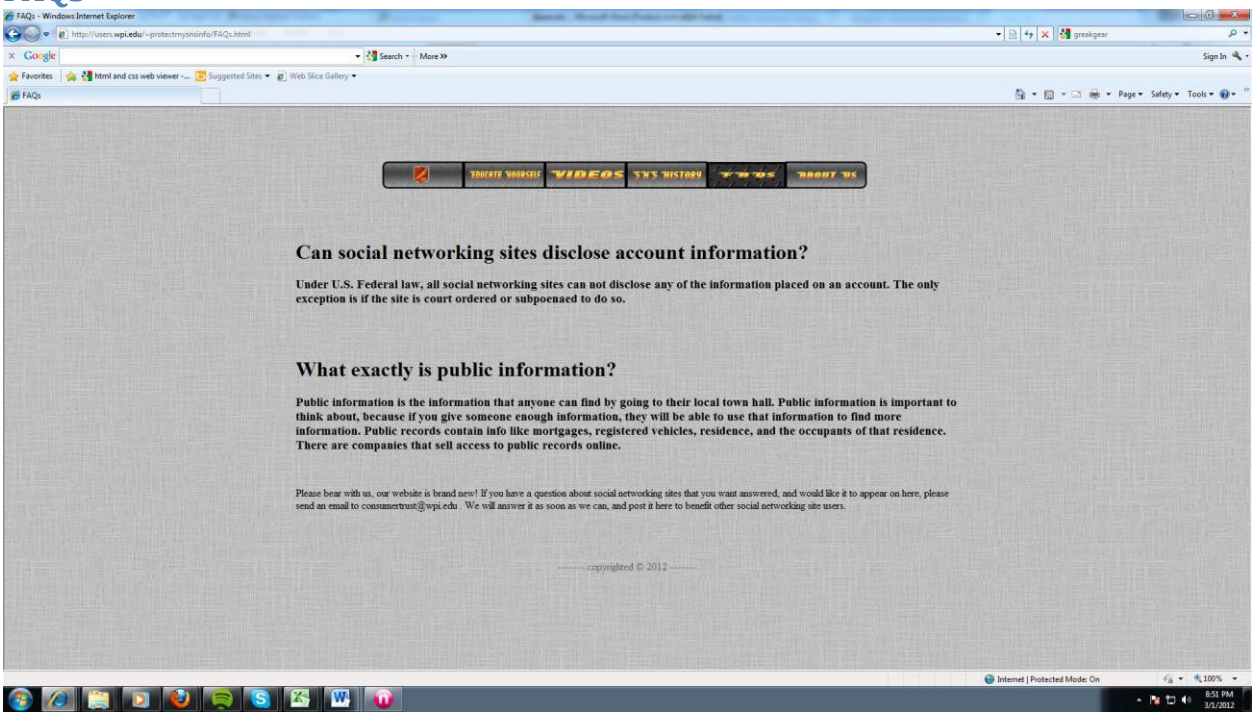
The videos tab links the visitor to all of our tutorial videos. We have four tutorial videos in total. They are Blocking a Person, Photo Album Protection, Status Update Protection, and Information Protection. Each of these videos recommend the other three videos when clicked on.

SNS History



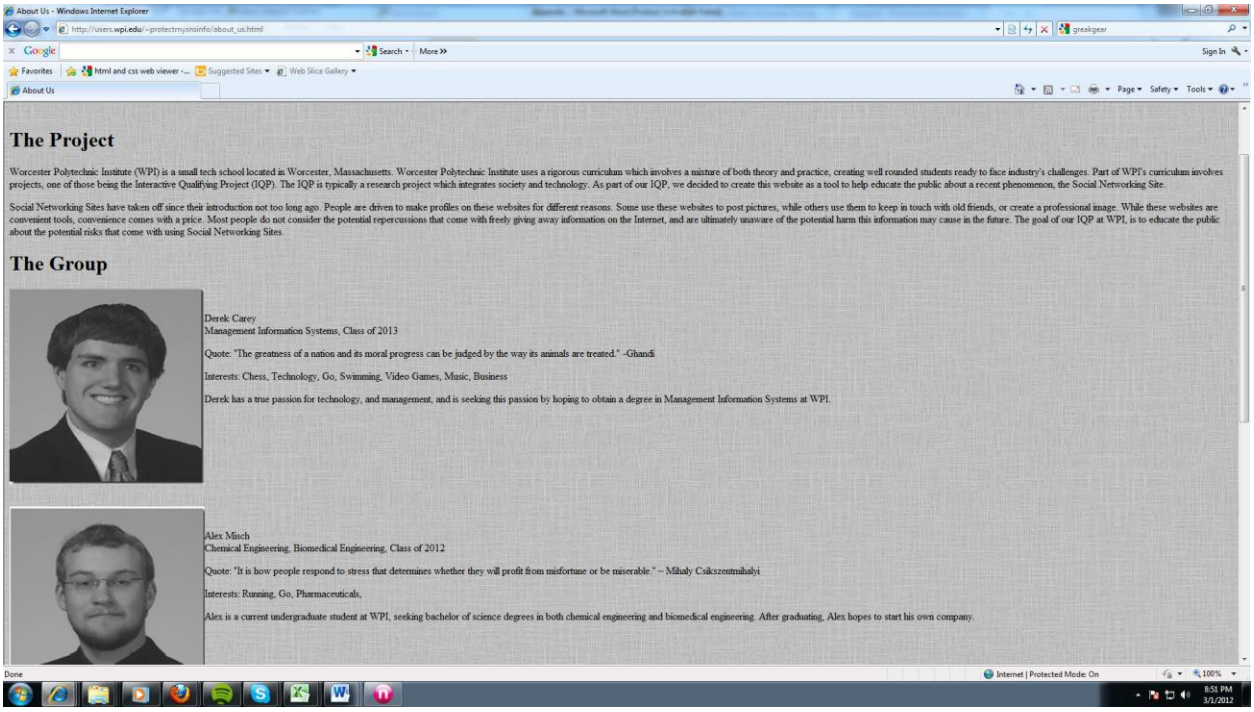
This page displays our social networking site timeline. On the timeline are famous social networking sites that have appeared throughout history. When clicked, each social networking site on the timeline loads information about that social networking site. Under the block of information for each social networking site, is an image that when clicked on brings the visitor to the source of the information.

FAQS



The FAQS page at this point in time is really a template for the future. Right now we have two questions, one related to public information, and the other asking if social networking sites can disclose your information. As the website grows in usage, then we will accept questions. As we answer these inquiries, we will add them to the FAQs page.

About Us



On the final page of our website, we discuss the project, and describe why we did it. Next, we post a picture for each member of the group, and then add some basic information about each member of the group.

The Implementation

Now that protectmysnsinfo has been created, it is important to spread the word about the website. In order to advertise the tool, we created a brochure. In order to view the brochure, please see appendix sdas. The brochure was designed, and sent to the communications group at WPI to be optimized. The final design will be printed, and dispersed to every major building on campus. The brochure was designed in a colorful manner in order to quickly grab the passerby's attention, and suggest the reader browse to our website. While we mainly designed the website with new WPI students in mind, we want to make the WPI campus aware of our project.

Through Mr. Spellman's workshops, and the distribution of our brochures, we will be able to quickly spread news of our website.

Future Plans

The creation of protectmysnsinfo is just the beginning. During the first few years, it is crucial to receive feedback, and optimize the website. Besides optimizing the website, it is crucial to make the program as strong as possible. Once these two conditions are met, then the next logical step would be to spread the program to other colleges.

As fulltime students, a problem quickly arises. The typical IQP at WPI is 3 terms in duration, the equivalent of 21 weeks. After the duration of this project expires, each member of the IQP will move on to other course loads, and the Major Qualifying Project (MQP). Once the project is completed, the source code for the website will be handed over to Mr. Neil Spellman, along with the brochure design. For the first few months of the website's implementation, the group will accept feedback, and make necessary fixes. By going through this process, we will ensure that we leave WPI with a strong product that they will only have to make minor edits to with time once we graduate.

Works Cited:

1. Amichai-Hamburger, Yair, and Gideon Vinitzky. "Social Network use and Personality." Computers in Human Behavior 26.6 (2010): 1289-95. Web.
2. Antony, Solomon, Zhangxi Lin, and Bo Xu. "Determinants of Escrow Service Adoption in Consumer-to-consumer Online Auction Market: An Experimental Study." Decision Support Systems 42.3 (2006): 1889-900. Print.
3. Boyd, Danah M., and Nicole B. Ellison. "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13.1 (2008): 210-30. Print.
4. Cao, Alice, and Mark Kochanski. "Facebook and US Privacy Policy." *Facebook and US Privacy Policy* (2010): 1-18. Print.
5. Cho, V., & Hung, H. The Effectiveness of Short Message Service for Communication with Concerns of Privacy Protection and Conflict Avoidance. *Journal of Computer-Mediated Communication*, 250-270. (2011).
6. Compeau, D., & Higgins, C. Computer Self-Efficacy: Development of a Measure and Initial Test. *Management Information Systems Research Center*, 189-211. (1995).
7. Crepeau, Neicole M. "Facebook Users: Goals and Time Spent by Age, Gender, Work Status, and Parental Status." Coherent Social Media. 19 June 2009. Web. 09 Oct. 2011. <http://blog.coherentia.com/index.php/2009/06/facebook-users-study-of-facebook-goals-for-differing-demographics/>.
8. Correa, Teresa, Amber Willard Hinsley, and Homero Gil de Zúñiga. "Who Interacts on the Web?: The Intersection of Users' Personality and Social Media use." Computers in Human Behavior 26.2 (2010): 247-53. Web.
9. Dwyer, Catherine; Starr Hiltz, and Katia Passerini. "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace." Association for Infomation Systems: 1-13. Print.
10. Dwyer, Catherine. "Digital Relationships in the 'MySpace' Generation: Results From a Qualitative Study." Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS): 1-10. Print.
11. Fogel, J., and E. Nehmad. "Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns." Computers in Human Behavior 25.1 (2009): 153-60. Print.
12. Gonzalez. "Facebook Marketing Statistics, Demographics, Reports, and News." CheckFacebook.com. 25 Sept. 2011. Web. 09 Oct. 2011. <http://www.checkfacebook.com/>.
13. Ralph Gross and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (WPES '05). ACM, New York, NY, USA, 71-80
14. Hsi-Peng Lu, Kuo-Lun Hsiao, The influence of extro/introversion on the intention to pay for social networking sites, Information & Management, Volume 47, Issue 3, April 2010, Pages 150-157. (http://www.sciencedirect.com/science/article/pii/S0378720610000042)
15. Jones, Kiku, Lori N. K. Leonard, and Cynthia K. Riemenschneider. "Trust Influencers on the Web." Journal of Organizational Computing & Electronic Commerce 19.3 (2009): 196-213. Web.
16. Michael D Kaplowitz, Timothy D Hadlock, and Ralph Levine. "A COMPARISON OF WEB AND MAIL SURVEY RESPONSE RATES." Public Opinion Quarterly 68.1 (2004): 94-101. Print.
17. Kenyon, Henry S. "Cybercriminals Find New Ways to Exploit Vulnerabilities." Armed Forces Communications and Electronics Association (2010): 23-27. Print.
18. Kiehne, Thomas P. "Social Networking Systems: History, Critique, and Knowledge Management Potentials." *Social Networking Systems: History, Critique, and Knowledge Management Potentials* (2004): 1-23. Print.
19. Kim, Byoungsoo; Han, Ingoo. "The Role of Trust Belief and Its Antecedents in a Community-Driven Knowledge of Environment." Journal of the American Society for Information Science and Technology (2009): 1012-1026.
20. Kim, Dan J. "Self-Perception-Based Versus Transference-Based Trust Determinants in Computer-Mediated Transactions: A Cross-Cultural Comparison Study." *Journal of Management Information Systems* 24.4 (2008): 13-45. Print.
21. Kim, Dan J., Donald L. Ferrin, and H. RaghavRao. "A Trust-based Consumer Decision-making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents." Decision Support Systems 44.2 (2008): 544-64. Print.

22. Krasnova, Hanna; Kolesnikova, Elena; and Guenther, Oliver, ""It Won't Happen To Me!": Self-Disclosure in Online Social Networks" (2009). *AMCIS 2009 Proceedings.* Paper 343. http://aisel.aisnet.org/amcis2009/343
23. Kuan, Huei-Huang, and Gee-Woo Bock. "Trust Transference in Brick and Click Retailers: An Investigation of the before-Online-Visit Phase." Information & Management 44.2 (2007): 175-87. Web.
24. Kuan-Yu Lin, Hsi-Peng Lu, Why people use social networking sites: An empirical study integrating network externalities and motivation theory, Computers in Human Behavior, Volume 27, Issue 3, May 2011, Pages 1152-1161. (http://www.sciencedirect.com/science/article/pii/S0747563210003766)
25. Kwak, Haewoon, Changhyun Lee, Hosung Park, and Sue Moon. "What Is Twitter, a Social Network or a News Media?" *What Is Twitter, a Social Network or a News Media?*: (2010)1-10. Print.
26. Landman, Matthew P., et al. "Guidelines for Maintaining a Professional Compass in the Era of Social Networking." Journal of surgical education 67.6 (2010): 381-6. Print.
27. Livingstone, S., & Helpser, E. "Balancing Opportunities and Risks in Teenagers' use of the Internet: The Role of Online Skills andInternet Self-Efficacy." *New Media and Society*, 309-330. (2010).
28. McGraw, K. O., & Wong, S. P. (1992). A common language effect-size statistic. Psychological Bulletin, 111, 361-365.
29. Patchin, J. and Hinduja, S. "Trends in Online Social Networking: Adolescent Use of MySpace Over Time." *New Media Society*, 197-216. (2010).
30. Jeffrey Pomerantz, and Frederic Stutzman. "Collaborative Reference Work in the Blogosphere." Reference Services Review 34.2 (2006): 200-12. Print.
31. Reynolds, Rodney, Robert Woods, and Jason Baker. "Handbook of Research on Electronic Surveys and Measurements (9781591407928): Rodney A. Reynolds, Rodney A. Reynolds; Robert Woods; and Jason D. Baker: Books." *Google Scholar*. Web. 31 Aug. 2011.
32. Ross, Craig, et al. "Personality and Motivations Associated with Facebook use." *Computers in Human Behavior* 25.2 (2008): 578-86. Print.
33. Stewart, Katherine J. "Trust Transfer on the World Wide Web."*Organization Science* 14.1 (2003): 5-17. Print.
34. Worcester Polytechnic Institute, Division of Enrollment Management. "2010 Factbook." 2010 < http://www.wpi.edu/Images/CMS/Bartlett/Factbook_2010(2).pdf>
35. Zywica, Jolene, and James Danowski. "The Faces of Facebookers: Investigating Social Enhancement and Social Compensation Hypotheses; Predicting Facebook? and Offline Popularity from Sociability and Self-Esteem, and Mapping the Meanings of Popularity with Semantic Networks." Journal of Computer-Mediated Communication 14.1 (2008): 1-34. Web.
36. LinkedIn. "About Us." *LinkedIn Press Center*. 2012. Web. 10 Jan. 2012. <http://press.linkedin.com/about>.
37. Papacharissi, Zizi. "The Virtual Geographies of Social Networks: A Comparative Analysis of Facebook, LinkedIn and ASmallWorld." *New Media & Society* 11.1-2 (2009): 199-220. Print.
38. Google. "Google+." *A Quick Look at Google+*. 2011. Web. 11 Jan. 2012. <http://www.google.com/intl/en/+/learnmore/>.

Appendix 1: Meeting Minutes by date

Meeting 8PM Wednesday September 21st, 2011

Attendance
Present:
Richie
Derek
Misch

Not Present:
Anthony – Has a musical

Group Discussion: Complete online IRB course
Talk about WPI's demographics
What can we expect for sample sizes
Contact Stacy Swartz for help with research, control and sampling
Edit literature review so far
Work on methodology
Methodology – introduce an ideal situation, introduce our situation
Put more thought into survey questions
Methodology – introduce an ideal situation, introduce our situation

Action Items:

Derek: Read and annotate magazine article from Professor Loiacono
Methodology
Take online course

Anthony: History/Background of social networking
Take online course

Richie: Look at survey questions for hypothesis
Look up WPI demographics
Research on survey sample sizes
Email Stacy Schwartz
Write up on WPI demographics, methods of searching for subjects (ex. email
or personal searching by word-of-mouth?)
Take online course

Misch: Methodology
Proofreading
Take online course
Create agenda for meeting on friday

Meeting 9/25/11
Start Time: 11:31 AM

Attendance: Misch, Anthony, Me, Derek

Discussion:
Project Title
Currently cyber-security
Consumer trust in social networking sits
- Problem – trust is only one aspect

Self-Disclosure on Social Networking Sites

Slide Show Presentation for Tuesday meeting
Survey constraints, WPI, Worcester Colleges? Boston Colleges?
Narrow to WPI
Anthony and Misch need to finish online course
Change email alias from cryptography@wpi.edu to something more suitable.
Work on writeup and provide for Professor for this upcoming weekend
Make questions for Fisler
Concept Paper
Setup the dropbox
RefWorks

Respond to Laura Hanlan for meeting
After 3pm Wednesday
4pm Tuesday
4pm Friday

Action Items:

Group: Meet with Professors Loiacono and Fisler on Tuesday, 11am

Richie: Email professors Loiacono and Fisler confirming meeting on Tuesday
Email Laura Hanlan for meeting in library
Make survey questions for hypothesis
Revise Demographics doc

Anthony: Background (add Facebook/other functions)
Finish online course
Make questions for hypothesis

Alex: Make questions for hypothesis
Edit presentation
Editing Paper
- Make list of what needs more research

Make Agenda for 9/27/11

Meeting Friday October 7th, 2011
9:11PM

Attendance:
Present: Richard Speranza, Alex Misch, Anthony Spencer, Derek Carey
Not Present: N/A

Business Items:

Filling out the IRB form

Compensation

- Desserts at campus center during lunch? Possible table sit
- Grand Prize idea
- Pizza
- First # of people ….. get ……
- No Compensation?
  This makes the most sense, if we compensate we will need to collect personal information

Send a preliminary survey to the undergrad alias

Reviewing Survey Script

Making edits to compiled paper so far, finding WPI IQP format. Added table of contents, cover page. Adding Page Numbers

Updated model – Computer self efficacy -> Social Network Self Efficacy
Reputation -> Consumer Reputation

Action Items:

Derek: Smart PLS, Write intro to model, limitations, other placeholders **Misch:**
Survey Script, email professor Loiacono IRB draft from this meeting **Richie:**
Format paper, post minutes, import sources to RefWorks, update model
Anthony: Fix consent form, Conclusions, update model

10:30PM

Minutes for Meeting Wednesday October 26th, 2011
Start: 8:51PM

Attendance:
Present: Richie, Misch, Anthony, Derek
Not Present:

Old Business:
Edit your individual sections of paper based off of Professor's corrections
Survey Incentives

New Business:

Going over how to track changes

- Review -> Track Changes
- Put in comments, different colors and initials for each user

Set up When2Meet Website for B-term

Change numbering for flow chart

- Counter clockwise outside circle
- Write transitions

Action Items

- Richie – track changes to portion of paper, make sure transitions have been written, change numbering of model hypothesis, when2meet
- Anthony – track changes to portion of paper, make sure transitions have been written, move order of hypothesis in paper based off model changes, when2meet
- Misch – track changes to portion of paper, make sure transitions have been written, when2meet
- Derek – track changes to portion of paper, make sure transitions have been written, when2meet, make meeting agenda

Meeting End Time 9:43 PM

IQP meeting minutes
Monday November 7th, 2011
Start Time: 11:05 PM

Attendance: Richie, Derek, Misch, Anthony

Old Business:

- Document Edits

New Business

Update powerpoint presentation
- Dress code tomorrow – suits

Consolidation Doc edits
- Need to combine everyone 's edits

Changes to title page
- In partial fulfillment of _____
- Signatures

Action Items:

Enhance survey
Finish presentation, present
Combine paper revisions

End time: 12:10PM

IQP Meeting
Sunday December 4th, 2011
Start Time: 7:50 PM

Attendance:
Present: Misch, Derek, Richie, Anthony
Not Present: None

Paper Edits:

- Take the paper from dropbox -> make your edits.
- Email it to the next person when you are done editing it
- Track your changes

Paper Edits Schedule:
Misch make edits give to Derek for Tuesday morning
Derek send to Richie for Wednesday night
Richie send to Anthony for Friday at noon
Misch then does final revisions -> then send it back out (put it back on dropbox)

Survey Update:
Survey sent out on Thursday December 1st, 2011, pending SGA approval to be distributed to the undergraduate body.
If the survey doesn't get sent out by tomorrow at noon, Anthony will contact SGA

Meeting End Time 8:20

Meeting Minutes December 12th, 2011
Start Time: 8:15PM

Attendance
Present: Richie, Antony, Misch, Derek
Not Present: None

Discussion:
- Editing Paper
  - Edits half done, more work will be done after finals
- Survey Results
  - 570 people attempted, 370 people survived
- Website
  - Anthony spoke with helpdesk to get a website set up on the wpi server
  - protectmysnsinfo.wpi.edu
  - want basic information in order to set up the site
  - giving professor's username so the website stays after we graduate, but we will still be able to edit the website (primary and secondaries)

TO DO LIST:
- Finish initial edits
- Add plan for results
- Figure out smart PLS and do initial testing – gather questions
- Videos for the website?
- Learn how to make website look really nice
- Make appointment with Neil Spellman and Kerrie O'Connor

Questions:
- When can we close the survey?
- Can we delete unfinished data?

Minutes 1/11/12
Start Time: 7:32 PM

Attendance: Richie, Anthony, Derek, Misch

New Business:

IQP Edits:

Anthony sends edits to Misch by next meeting
Sometime next week meet as group accept changes to paper

Website

HTML or wordpress?
Wordpress is easier but more blog oriented
Html is more complex but delivers a more professional product

Data

Filter out data (some people put their names/didn't really answer questions)
SmartPLS analysis

Questions:

What needs to be done for the final product? Does it have to be revised for a journal?

End Time: 8:15 PM

Minutes for Meeting Wednesday January 12th, 2012
Start: 12:00PM

Attendance:

Present: Anthony, Richie

Old Business:

Get Group account to work for the IQP group
Website Domain is now www.wpi.edu/~protectmysnsinfo

New Business:

Website Design Outline

Home:

a. A nice cool pictures with all the different logos of the SNS sites.
b. A tag line like "do you know how to protect yourself
c. Talk about the motivation for doing this project

Educate Yourself:

a. Java Script for interactive learning tool. (Figure out what to do)

Videos:

a. Split up into different SNS sites.
    i. Facebook
        1. Privacy Settings
            a. Block individuals
            b. Block groups
            c. limit the amount of viewer
            d. public/private profile
    ii. Twitter
        1. Privacy Settings
            a. Limit the amount of followers
            b. public/private
    iii. LinkedIn
        1. Privacy Settings
    iv. Google+
        1. Privacy Settings

b. Get someone with a cool voice to do the voice over
c. make a cool intro for videos

d. make a cool exit for videos
e. Date videos incase the SNS site changes

SNS History:

a. Use SNS Background from paper to give a nice brief history.
b. Use images to make it easier to understand

Research Summary:

a. Overview of steps we took to do research.
b. Display data all on this page for easy reference
c. Put Model in and explain it clearly

Presentation:

a. Put up final presentation for viewing because it will be nice to reference.

About Us:

a. Pictures of each person
b. Blurb about each person
c. Emails for contact for further questions

Miscellaneous:

a. Page Background Pictures
b. Sounds

Action Items:

Anthony - SNS History Page, Video Intro and Video exit, Find someone with a cool voice
Richie - About Us Page, Motivation on Home Page, Find someone with a cool voice

Meeting End Time: 1:30 PM

IQP Meeting 2/26/12

Attendance: Misch, Anthony, Richie, Derek

Paper:

Status- sent to professor to be edited, almost finished. Paper is due second day of D term.

Need to upload materials to appendix
Need to write more for paper about website
Need to update omnigraffle charts

Reputation needs to be changed. Sites reputation in survey, but consumer reputation. Delete or edit in paper?'

Need to give out visa gift card

Website:

Put copyright on bottom of each page

Tutorials are done

Remove research summary and presentation

Website is basically finished

Powerpoint:

Meet Wednesday night to do powerpoint

Action Items:

Derek – Methodology section, edits, give professor survey data

Misch – Add abstract and executive summary, compile appendices, edits, reserve tech suite for Thursday at 1pm.
Appendices – meeting minutes, brochure, survey questions,

Richie – Write up about website, compile source code

Anthony - compile source code, add copyrights, fix toolbar, upload videos, send me screenshots

IQP Meeting 2/29/12

Attendance: Misch, Anthony, Richie, Derek

Final Presentation is tomorrow

1.) Delete line from consumer reputation to perceived benefit
2.) Change consumer reputation to reputation and add a line from that to consumer trust

For perceived benefit and Intention to Disclose, expand personality type into all 5

Paper needs to be edited

Need appendixes

Executive summary
Abstract

Make sure conclusion and discussion make sense

Finalize for submission

Presentation
Misch has introduction – each introduce self
Misch does project objective slide
Anthony talks about social networking site definition and timeline
Derek – Introduce Model, Then discuss each slide
Misch – Research Demographics

ADD TO PRESENTATION
Talk about survey – responses, release date, (DEREK MAKES SLIDE)
Talk about how results were found – SPSS – linear regression model and why (DEREK)
Results of data – pictures of results, and r squared values. What held/what didn't hold? (MISCH)
Conclusions – implications of the data and lessons learned (MISCH)
What are we doing to impact society? (MISCH)

- Talk about findings and how it will impact society – people's perceived risk varied a lot, not a consistent level of education when talking about disclosing information

Website (RICHIE – pamphlet stuff, NSO, volume)

- Pass out pamphlets, talk about new student orientation
- Go into website

Richie – Introduction to the website, explain why we're doing it etc.
Go into educate yourself, explain how its interactive, talk about links to sites, and test

Anthony – tutorials, SNS history, FAQS, about us

Derek – Do wrap up - Acknowledgements (DEREK MAKE SUMMARY SLIDE, Richie make acknowledgement slide)

Questions (ANTHONY/RICH)

4 slides with results and conclusions (DEREK/MISCH)
1 slide with the entire model (ANTHONY/RICH)

** DEADLINE FOR SLIDES IS 2AM **

Change consumer reputation to reputation
FIGURE OUT LINKS FROM THERE

Derek – finalizing paper, get flashdrive WEBSITE SOURCE CODE, WEBSITE ACCOUNT AND PASSWORDS, SURVEY QUESTIONS, SPSS DATA, SURVEY DATA, PAPER,

Misch – Give Richie names for personality types from paper, change 5 factor model name to agree between lit review and discussion

Richie – Add source code to appendix, make new models

Anthony – compile slides

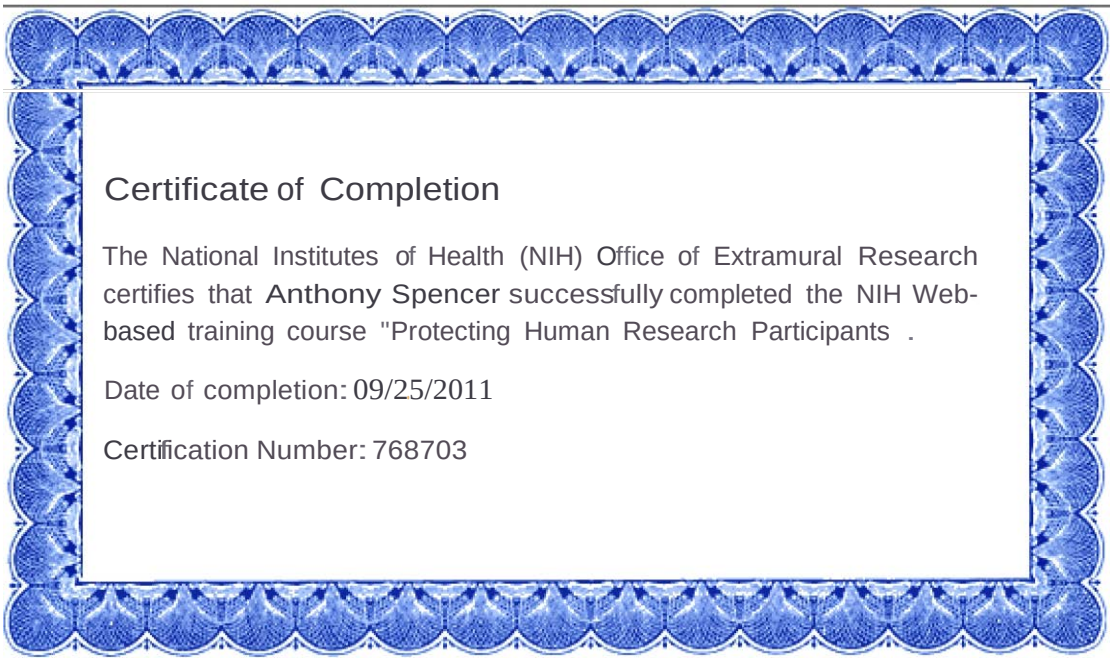
Appendix 2: IRB Research Certificates

Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that Alexander Misch successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 10/11/2011

Certification Number: 784604

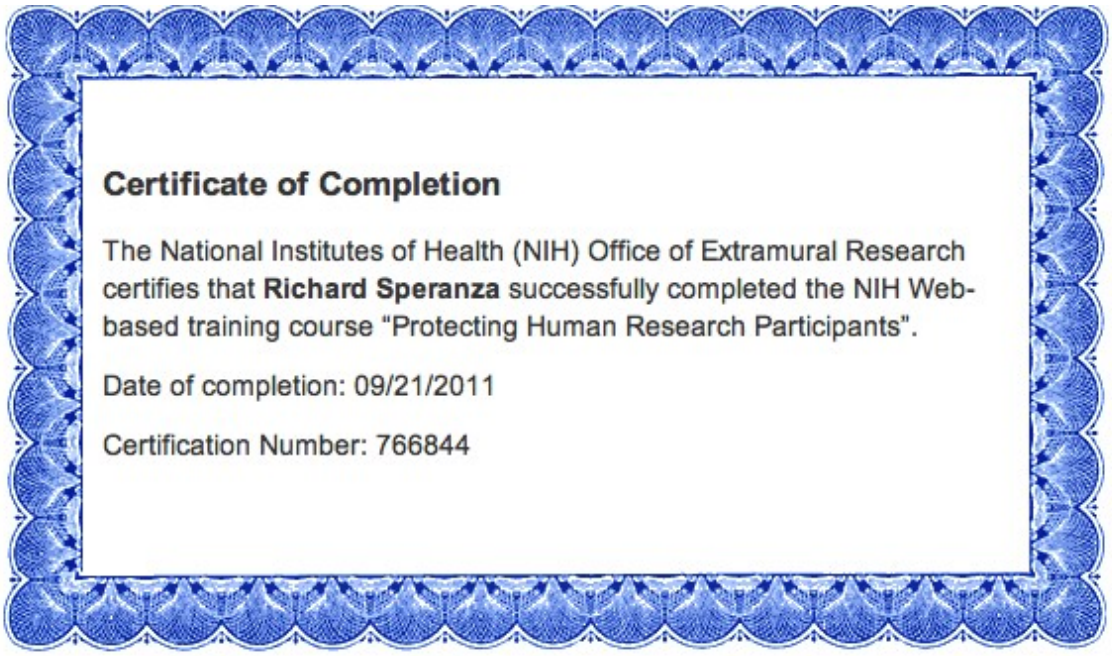


Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that Anthony Spencer successfully completed the NIH Web-based training course "Protecting Human Research Participants .

Date of completion: 09/25/2011

Certification Number: 768703



Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Richard Speranza** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 09/21/2011

Certification Number: 766844

Appendix 3: WPI Informed Consent Statement

WPI INFORMED CONSENT STATEMENT FOR
INFORMATION SELF-DISCLOSURE STUDY

STUDY PURPOSE:
This research project is on consumer information disclosure on Social Networking Sites. We are interested in what exactly affects a person's decision to disclose their information online. You are invited to participate in this study. You will be asked several questions to gauge how information is disclosed. This survey shouldn't take any longer then 30 minutes.

NUMBER OF PEOPLE TAKING PART IN THE STUDY:
If you agree to participate, you will be one of approximately 150 subjects who will be participating in this initial research.

PROCEDURE FOR THE STUDY:
If you agree to be in the study, you will be asked to do the following things:
Answer a few questions about yourself.

- Answer questions about your experience with Social Networking Sites.

Note: If you feel uncomfortable once you begin the study, you may stop participating at any time.

RISKS OF TAKING PART IN THE STUDY:
The reduction of risk in association with your participation has been taken very seriously. With any experimental study, like this one, there can be a risk of a loss of confidentiality. To minimize this risk, your answers will be kept confidential and only associated with a subject code number. This subject code number will not have any individual identifier, as it will be randomly generated. This means that your name will never appear on any questionnaire or any of the results found. We do not expect any of the risks to occur; however every precaution that is necessary will be taken to prevent them. Protocols have been developed to prevent data management errors. Data will be stored in a closed and locked location.

BENEFITS OF TAKING PART IN THE STUDY:
Your participation in this research will be most helpful in understanding how people decide to disclose their information on Social Networking Sites.

CONFIDENTIALITY:
Maintaining your personal information confidential is very important. Efforts will be made to keep this personal information private. We cannot guarantee absolute confidentiality. If requited by law. your personal information will be disclosed. Your name will not appear in reports in which the study maybe published.
Organizations that may inspect and/or copy your research records for quality assurance and data analysis include groups such as the investigators and their research associates, and the WPI Institutional Review Board (IRB) or its designees.

COSTS/COMPENSATION:
Physical injury due to participation in this study is highly unlikely. However. in the event you do endure physical injury because of your participation, necessary medical treatment will be provided to you and billed as part of your medical expenses. Any costs not covered by your health care insurer will be your responsibility and not that of the researchers or Worcester Polytechnic Institute. Also. it is your responsibility to determine the extent of your healthcare coverage. There is no program in place for other monetary compensation for such injuries. However, you are not giving up any legal rights or benefits to which you are otherwise entitled. On a brighter note, you will receive free cookies with your participation in this study.

CONTACTS FOR QUESTIONS OR PROBLEMS:
For questions about the study, contact the researchers, Eleanor Loiacono (508-831-5206, eloiacono@wpi.edu), Derek Carey (dac52991@wpi .edu). Alex Misch (misch_alex@wpi.edu). Anthony Spencer (anthony_spencer@wpi.edu), or Rich Speranza (rsperanza@wpi .edu).

VOLUNTARY NATURE OF STUDY:
Taking part in this study is voluntary. You may choose not to take part or may leave the study at any time. Leaving the study will not result in any penalty or loss of benefits to which you are entitled.

CONSENT:

I certify that I have read and understand the foregoing, that I have been given satisfactory answers to my inquiries concerning project procedures and other matters and that I have been advised that I am free to withdraw my consent and to discontinue participation in the project or activity at any time without prejudice.

I herewith give my consent to participate in this project with the understanding that such consent does not waive any legal right nor does it release the principal investigator or the institution or any employee or agent thereof from liability for negligence or for any wrongful act or conduct.

_____	_____	_____
Name (please print)	Signature	Date

If you cannot obtain satisfactory answers to your questions or have comments or complaints about your treatment in this study, contact: Kent Rissmiller, the chair of Institutional Review Board (IRB) at WPI, Atwater Kent 124, Phone: 508-831-
5019, Fax: 508-831-5896, email: kjr@wpi.edu.