PERSONAL INFORMATION IN PUBLIC DOMAIN: PERCEPTIONS OF RISK AMONG COLLEGE STUDENTS ON FACEBOOK AND THE OUTSIDE WORLD

Kayla Picotte

A Thesis Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Arts

Department of Sociology and Criminology

University of North Carolina Wilmington

2012

Approved By

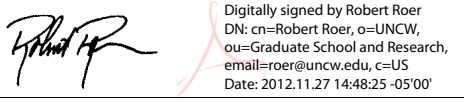
Advisory Committee

Sangmoon Kim

Michael Maume

Cecil Willis
Chair

Accepted by



Dean, Graduate School

TABLE OF CONTENTS

ABSTRACT

The use of social media websites, specifically Facebook©, by college students was used to draw a connection between students' perception of crime and potential victimization and the personal information they post in public forums. This paper attempts to determine if the perception of physical and online risk has any influence on students' likelihood of providing private and identifiable information or using privacy settings on a publicly visible social networking site. A random sample of 3,000 students was drawn from a large public university and given a link to an online survey that measured physical and online risk perception, as well as the level of information disclosure on Facebook© (n=646). While it was found that majority of students do not post information such as their address and phone number, there are gender differences and differences regarding the number of friends one has. Overall, online perception of risk does predict most of the sharing students do on Facebook©, but the link between risk perception and information disclosure is not a clear one, with factors such as age and past history with victimization also appearing significant.

LIST OF TABLES

INTRODUCTION

College students today have more opportunities than ever before to present and manage their social image before an ever-increasing audience with the help of online social networking sites (SNS). One of the most popular social networking websites in the world, Facebook.com, came from humble beginnings in a Harvard University dorm room, engineered by a student whose name has now become a household staple. In 2004, Mark Zuckerberg launched Facebook© as an online yearbook for students to upload pictures and descriptions of themselves as a way to stay in touch through college networks. Originally it was only open to students with a college e-mail address, but in 2007 Facebook© became available to anyone who wished to sign up. By 2010 Facebook© had over 500 million members from all across the globe, allowing the exchange of information to create an unprecedented social world (Richmond 2010). These sites create a virtual index of information about individuals unprecedented in the modern social world. No longer do you actually need to contact someone to find out what is going on in their life, you only need access to their Facebook© page. The benefits to this new arena of social interaction seem to be endless – networking with classmates is now a breeze, it's easy to keep in touch with long lost friends and even employers are using it to gain recognition and scout out potential employees.

Facebook© had grown in popularity so quickly that concerns about privacy issues and the potential danger of divulging such personal information online barely had time to surface. Originally the threat level was seen as low, as only other college students within the same online network could view a member's profile. Once the site was available to minors, advocacy groups expressed concerns about the dangers of online predators using

the site to find potential victims. The Center for Missing and Exploited Children cites the Internet as one of the main avenues that predators use to target minors, and provides guidelines about posting personal information on social networking sites (tcs.cybertipline.com). It was becoming clear that while there are serious issues and risks associated with divulging private information in a public forum, the desire to act on this new sociological stage and to reach an unlimited audience has significant power over those engaging in it. While college students are no longer minors, they still may be putting themselves at risk by making personal identifying information available in public domain.

The most alarming aspect of Facebook© and other social networking sites was that all of the information was voluntarily provided. "To create the profile, the new member is asked to fill out forms with identifying information such as name, age/birthday, gender, hometown and/or location, religion, ethnicity, personal interests, contact information and an 'about me' section. Most SNS also encourage users to upload a profile photo" (Taraszow*et al.* 2010: 83).While almost all social networking sites allow various levels of privacy controls and allow users to control who can view which parts of their profile, the default visibility level for Facebook© was originally set so everyone in the "network," that is, everyone in the college for a college student, could view them (Tufekci 2008). When the site changed to allow all users to sign up, those settings automatically shifted so that every users'profile was visible to all others if they did not manually change the settings (Taraszow*et al.* 2010). In the early years when the voices of privacy concern were quieter, it was very possible that users were not even aware how many people could view their profile or that they had the ability to limit it. Thus there a standard of information disclosure on the website was established that continued even after privacy concerns were

raised and a norm was established among users that a certain level of disclosure was expected in order to maintain the social experience.

My main research hypotheses focus on the perception of physical and online risk and how that may predict the disclosure of information on Facebook©. These will be tested by creating a scale to measure perception of risk in physical and online scenarios, analyzed with students' use of Facebook© and how they monitor their information online. Level of information disclosure will be analyzed against several independent variables including basic demographics (sex, age, race) and other possible control factors that could influence a student's behavior on Facebook© (such as a parent or professor having access to their profile). Drawing a link between how students are interpreting environmental cues that may put them at risk and then how they choose to react to those scenarios (making themselves more or less vulnerable) could help parents and schools better understand this environment and educate students on the dangers of disclosing too much.

LITERATURE REVIEW

Recent studies have found that Facebook© membership among college students is consistently high, with around 90% of those surveyed indicating use of the site (Christofides, Muise and Desmarais 2009; Tufekci 2008). With such widespread use, educators became concerned with the level of exposure displayed on the site. Almost all students used their real name, 83% listed their relationship status and even 16% posted their cell phone number (Tufekci 2008). Distressed by these findings, college administrations began to create task forces that were assigned to develop educational programs to assess and strengthen students' knowledge of the potential consequences

regarding the use of social networking sites (Kite, Gable and Filippelli 2010). As Facebook© started to gain nationwide recognition for this concern, threats of predation through social networking sites and instant messaging programs started to stir numerous problems for parents, school administrators, and law enforcement on a national level (Kite, Gable and Filippelli 2010). There seemed to be a new social realm emerging for young people with a steep learning curve, one that had inherently different rules and understandings about standards of privacy and control. The Internet provided an endless outlet for disclosure but no perception of an immediate threat.

In addition, "worrisome stories about identity theft and stolen credit card numbers began appearing regularly in newspapers and television news" (Tufekci 2008:20). These stories were linked to the online disclosure of personal information like that available on Facebook©. The security of Facebook© was being challenged in a very public way, so that students could now see that it was not only other college students viewing their profiles, but potential criminals. Stories surfaced of individuals whose homes were burglarized because the perpetrator knew they would not be home due to their schedule being posted on Facebook© (Thacker 2010). However, while student users of Facebook© certainly became more aware and did express concern for their online privacy, studies show it did not cause them to change their Facebook© sharing behavior (Lewis, Kaufman and Christakis 2008;Timm and Duven 2008).

With increased publicity and criticism of Facebook©'s attitude towards privacy, CEO Mark Zuckerberg responded by unveiling new and more sophisticated privacy controls on the website in May 2010. These more personalized options allowed users to completely filter all information posted about them and block certain people from viewing specific

aspects (Richmond 2010). In addition, it also changed default settings of "searchability" through Google and other search engines, which was a primary concern of advocacy groups. This temporarily stifled criticisms yet research has not explored the extent to which the new privacy controls are used. Some evidence shows that college-age students still think that their Facebook© activities are more private than they actually are (Grimmelmann 2009; Peluchette and Karl 2010).

However, even with new privacy settings in place most Facebook© users are aware that their social networking page is not impenetrable. As an online source it is vulnerable to hacking, in which a person (usually from a remote location) uses skill and knowledge of computer code to bypass the password protection on one's account and gains access to it without the account holder's knowledge. While the level of skill needed to accomplish this used to be relatively rare, it is becoming more common among university students who may learn such techniques in the classroom. Surveys that have inquired about the use of Facebook© by college students indicate that these incidents have been increasing. Often they are perpetrated by someone known to the victim who wished to cause distress and harassment by changing certain incriminating information on one's profile (such as a sexual preferences) (Debatin et al. 2009). This can be very damaging to a user's social life because typically when such changes to a profile are made they automatically become visible to all friends via the "News Feed."While this type of hacking may be seen as juvenile pranks, it is akin to identity theft on a smaller scale. When hackers take control of one's profile they can change all aspects of a person's image and potentially hold onto personal information after access is cut off. Statistics show that college/university age students, with a high frequency of online transactions fall into the highest-risk age category for identity

theft (Winterdyk and Thompson 2008). Beyond financial repercussions, the potential for emotional and social harm to the victim is great and has caused some users to delete their profiles altogether.

The intense popularity and risks of social networking sites then begs the question from social science, how do young people make the decision to disclose certain personal information? How do they view the online realm in terms of potential risk and what is the relationship between perception of risk and the use of privacy settings? Research into this relatively new field has so far found mixed results. Facebook© users seem more likely to perceive risks to others and not themselves, relaying the youthful mindset of "It won't happen to me." One survey of over 300 undergraduates found that, "despite recent media reports regarding the negative consequences of disclosing information on social network sites such as Facebook©, students are generally thought to be unconcerned about the potential costs of this disclosure" (Christofides, Muise and Desmarais 2009:341). Another found that Facebook©'s users under the age of 30 were actually more likely to use privacy settings as compared to those 30-65 and that the majority of young adult Facebook© users are engaged with managing their privacy settings at least to some extent (Boyd and Hargittai 2010). There currently is no consensus among studies as to how often privacy settings are utilized by young adults on social networking sites, or what prompts them to use those features. I propose that certain aspects of the Facebook© community may be acting to shift students' perceptions of risk and that, through an invisible and unique socialization process, they come to use different criteria than would normally apply to risk assessment to decide what information they should post.

Creating an Online Self

Negotiating identity and presentation of self in an online setting has become increasingly important for college students since it is now one of the main avenues for communication (Peluchette and Karl 2010). Sociologist Erving Goffman's main theories dealt with how individuals present themselves when confronted with an audience, and the different roles they can occupy during social interaction (Goffman 1959). He posited that individuals perform different social roles based on which situation they are in and how they interpret others will react to their behavior. Through the process of socialization they are taught that certain actions elicit certain responses from their audience, and thus we attempt to manipulate our audience into giving us the feedback we desire (Goffman 1959).

A student's presentation of self on Facebook© is therefore based on their interpretation of the norms associated with this space and what is expected of them as members of a university community. These expectations can be difficult to understand as they are communicated mostly through the data already present on the site and must be interpreted carefully from existing member's profiles. This can (and often does) happen through trial and error, with various consequences resulting from misinterpretation of the norms. In attempts to translate the image we wish to project to our audience, we take advantage of the site's many options for creative expression. Networks, photos, relationship statuses and preferences, personal beliefs and narratives are all at our disposal for manipulation into the perfect self. Although we may not get it right the first time, the beauty of having an online image is its malleability and the endless opportunity for revision and reinvention of self.

A successful interaction by Facebook© standards would include the addition of 'friends,' indicating to all users the positive reaction of your audience to the image you present. In order to become 'friends' with someone you must go to their page and request that your friendship be accepted. The possibility of denial is always present and can lead to serious devaluation of one's social experience offline as well as on the site. This can be seen as a form of audience rejection, much like Goffman discussed in a more traditional manner of being ignored or embarrassed in a physical interaction. Not only do you have the negative interaction between the actor and the audience member rejecting them, but a limitless crowd of bystanders can also witness the faux pas. Because it is possible to view a list of exactly who is friends with whom on Facebook©, getting rejected from a friend request may be akin to getting turned down for a date and having it publicly broadcast to millions.

The opportunity to have our pages publicly commented on via the 'wall' constitutes another important element of audience participation (Tufekci, 2008). Through this we see the creation of a primary and secondary audience, with the primary audience participating by actually commenting and writing on one's page, and the secondary audience viewing the comments posted but not interacting. This is an important distinction because although the secondary audience does not directly give feedback, they are able to judge the performance of one's profile based on the number (and content) of other posts. They are also completely invisible, with no way to track who has viewed the comments on one's page. However, they do have the power to use that information gathered from simply observing an interaction they were not part of by publicly evaluating it (and the participants) on their own page, making those judgments visible. Through social networking sites we are now given the

ability to judge one's performance not only on organic content but also by the size of the crowd already gathered and whether the assessment has been largely positive or negative. This has proved a crucial element for the presentation of self on Facebook©.

The ability to either post something directly to a person's wall or to send them a private message (much like an e-mail) can be seen as a front stage and back stage of interaction on the site. Recent changes to privacy settings also allow users to block certain parts of their profile from being seen by chosen individuals, groups or networks (Ibrahim 2008; Livingstone 2008). This creates infinite layers of front and back stage, as all of your profile may be open to a few people, but you have the ability to manage minute portions of your online image to specific people. For example, you can block all photos from a specific person or just certain albums, allow all but a few friends to see your relationship status and only have your phone number visible to a handful of users. Manipulations of privacy settings also come with their own set of expectations, such as if one's parents are members of Facebook© it is acceptable (and customary) to hide photos or posts from them (Mesch and Beker 2010).

This norm has appeared to stem from the tendency to post photos of illicit or illegal activity (such as underage drinking) that typically is hidden from parents. Although those who post these pictures are aware of the potential consequences, several common factors have been found that usually outweigh those risks. Here we see the same cultural values and expectations that exist in the physical social world being translated to a new online space. Underage alcohol consumption often gains one recognition and popularity within a social group among young people, however this can only occur if it is done publicly so others can view the effects. Facebook© has made that task much easier by featuring photo

uploads of virtually unlimited content to one's page (Christofides, Muise&Desmarais 2009). Now users need only to take a picture of them drinking (or engaging in other "popularity-building" activity) and post it to their page. Immediately their friends will be informed via the News Feed and instant reputation transformation begins to occur. This activity is purposefully hidden from certain parties, allowing for a more secretive creation of groups in the backstage where different interactions can take place, further shaping the online self.

These expectations become an even more general 'generalized other' because no longer can students actually know exactly who their audience is. The generalized other is described by Mead as an internalization of the attitudes, norms and values of a community that guide our behavior (Mead 1967). In a way, the site has allowed us to become even more objective when viewing ourselves because each time we log in we are confronted with our own page for evaluation. We can literally see ourselves the way others see us without the subjectivity of a mirror. This has powerful implications for how we view ourselves offline and within face-to-face social interactions. There has yet to be developed an application able to tell you exactly who is looking at your Facebook© profile, and therein lies the new complexity in presenting yourself to a "faceless" audience. This can be especially tricky if you are unsure how your information is being accessed and for what purposes, but that does not seem to bother most college-age students.

Although privacy settings are available, previous research has found that they are seldom used to the extent that they could provide any actual protection from potential economic or emotional victimization (Boyd and Hargittai 2010). This is where we come to address the concerns raised by privacy advocates and parents who worry that having personal information such as your full name, phone number, college and even address can

potentially make you vulnerable to crimes such as identity theft or harassment (Taraszow*et al.* 2010). The addition of the Facebook© 'News Feed' in the fall of 2006 provides the perfect example of how expectations of privacy and social image norms can be introduced, manipulated and ultimately internalized. When it was first launched the site was not yet open to the public and still dominated by college students. Before the News Feed came along you actually had to visit a user's page to view their activity, but with the News Feed all significant actions (such as new friend additions, changing relationship statuses, addition of photos etc.) made by friends were automatically displayed on one's home page when they logged in. This meant that the instant you did anything on Facebook© it was recorded and sent out to all friends as permanent evidence of action. Symbolically it made the social stage so large that you could never step off, even when you wanted to.

Initial reactions to this were overwhelmingly negative and it became popular to reject this new development with thousands joining "Anti-News Feed" Facebook© groups (Hoadley*et al*. 2009). It seemed that the privacy wires had finally been tripped and students were uncomfortable with this new breech of information. 55.5% of students actually said they were less likely to reveal information about themselves online after the News Feed was started (Hoadley*et al*. 2009). Zuckerberg responded by creating some new privacy settings surrounding disclosure via the News Feed, although to what extent they were used remains unknown. It seems that the concerns about the News Feed did not last because it continues to be a central part of Facebook©, illustrating how a community norm and value can be significantly changed over a short period of time even with backlash from members. In 2007 when Facebook© opened to everyone the News Feed fiasco was soon forgotten and new concerns were raised about minors on the site. It has now been

grandfathered in to those who started without it and the outcry appears to be over. Gradually, through this development, users became comfortable with the idea of being constantly on display and this attitude may have led to increased complacence when it comes to detection of online risk. In this way students are being socialized to behave differently in regards to their personal information based on Facebook's© unique community standards.

Perceptions of Risk: Online and Off

Within our everyday lives it is necessary to make constant assessments of personal risk regarding our behavior and action. Most consider this a vital learning process of childhood socialization where we come to understand cause and effect and that some effects are more desirable than others. "The recognition of certain situations or places as possessing potential danger of criminal victimization is what Ferraro (1995) calls perceived risk" (Mesch 2000:48). Risk is considered a personal perception that virtually all persons have an opinion on, even if they are actually unequipped with the information necessary to make a rational calculation (Ditton and Chadee 2005). With regards to criminal victimization, there are specific social and cultural values being communicated through institutions, education and media as to who is at risk and how they should protect themselves. Studies related to perception of risk and fear of crime have consistently found that women are more likely to perceive risk than men, and the young tend to perceive less risk than those who are older (Mesch 2000;Reid and Konrad 2004; Smith and Tortensson 1997).

Gender has been shown to be possibly the strongest predictor of feelings of risk and vulnerability, especially towards crime (Pain, 2001; Starkweather, 2007; Sutton and Farral, 2005; Franklin, Franklin & Fern, 2008). It is within this realm of socialization that we see strong gender stereotypes being continually perpetuated. Young girls learn to be wary of their behavior more so than young men because often the male is thought of as being the perpetrator (Pain, 2001). Women are more likely to receive cultural messages identifying them as weaker and less able to defend themselves against a potential attacker, resulting in an increase of female worry and anxiety. This has been referred to as an "ecological vulnerability" hypothesis, where women are socialized to believe they are inherently more at risk because of their sex while men are taught to discount risk and fear (Smith and Tortensson 1997). This has been shown to lead to significant efforts by women to police themselves and place strict limitations on where they can go and what they can do, especially when unaccompanied by men (Wilcox, Jordan and Pritchard 2007). While women may perceive themselves as more vulnerable due to gender, statistics show that men are more likely to be the victims of crime (Starkweather, 2007; Chadee, Austen and Ditton, 2007).

Although men and women perceive risk of criminal victimization differently, sources do indicate that this may be crime-specific. Women tend to be more concerned with the risk of sexual victimization, while men consider themselves to be most at risk for property crimes (Lane, Goyer and Dahod 2009;Reid and Konrad 2004). However, both of those types of victimization involve physical or tangible assault to persons or property, which occurs outside of an online interaction. A strong correlation has been established among women between the perception of risk and self-protection behavior in physical

situations (such as staying in groups, not going out at night, carrying a weapon for protection, etc.), but evidence of self-protective behaviors in online space is inconclusive. Some studies suggest that women are generally more concerned with their privacy on Facebook© and tend to take control by not only utilizing privacy settings but also deleting pictures and messages that reveal too much (Hoy & Milne 2010).

However, similar studies found that women are actually more likely to disclose certain information about themselves while men were not, such as personal preferences in music, literature and religion (Tufekci 2010). This may indicate a skewed perception of control and risk among Facebook© users, while they remain vigilant and concerned about specific information; they dismiss the potential risk of other disclosures. Social networking sites provide the opportunity for vast amounts of information exchange that could potentially be used to victimize users in the physical world, yet we see in some instances that the social benefits of the site seem to override any perceptions of risk (Christofides, Muise and Desmarais 2009). Is this space somehow different in that perceptions of risk from the outside world do not influence behavior, even though divulging such personal information clearly has the potential to cause harm offline?

Age is another very important factor when it comes to personal risk assessment and behavior based on this perception. It is typically found in research related to risk perception and assessment that the old perceive more risks than the young, despite statistics from the National Crime Victimization Survey that show the young are more likely to be victimized (Fisher et al. 1998). More recent studies that examine the relationship between victimization and age have shown that personal victimization peaks in adolescence and early adulthood and subsequently declines with age (Bureau of Justice

Statistics, 2006; Melde 2009). However, these studies presently account for only physical incidents of victimization and do not ask about related online activity. This disconnect may be shown directly in the use of social networking sites and the amount of personal information disclosed by young college students versus those who are older. A popular explanation for the disregard of risk among young college students is the newly found freedom they possess in a university environment and the temptation for constant social interaction at all costs (van Manen 2010). However it is important to point out that although age is a powerful predictor, it is often mediated by gender. Older men tend to perceive more risk than younger men while younger women show just as much concern as older women (Smith and Tortensson 1997).

Cultural Risk Theory: Explaining Perceptions of Risk

Assessments of personal risk are logically related to specific situations. For example one might perceive less risk at a party with friends as opposed to alone in a dark alley. One of the reasons why we perceive less risk when we are with those we know and trust or are in a familiar setting is related to our socialization and cultural values. In 1982 Douglas and Wildavsky formulated what came to be known as 'Cultural Risk Theory,' which still dominates much of the research done on risk in social science (Rippl 2002). Although somewhat difficult to test empirically, this theory stresses the cognitive aspect of risk assessment, as opposed to fear, which is emotionally based. The way we are socialized to consider certain people, places and situations as safe and others as potential dangers, reveals our socialization and how we define our surroundings.

In this view, culturally shared understandings and viewpoints are very important, as they help us define what is threatening and how we should react to it. “Douglas and Wildavsky (1982) developed the four prototypical cultural types using two central dimensions of sociality: control (grid) and social commitment (group)” (Rippl 2002:149). This grid produces four distinct cultural types that assess and respond to risk differently based on how they relate to control and social commitment. Of the four types, those who identify as “individualists” would be most likely to be involved with social networking sites, as they perceive risk as opportunity and see more benefits than danger in technology.

Related to and within Cultural Risk Theory are several subsets attempting to explain why individuals take the risks that they do. “Knowledge theory” posits that people worry most about the risks that appear to threaten them most directly and tend to screen out less immediate dangers (Wildavsky and Dake 1990). Social networking easily fits within this framework, as the detachment of the computer screen may allow the user to distance themselves from any feelings of danger. Consequences such as stalking or identity theft become an abstract threat because the perpetrator has no face; there is nothing concrete to be afraid of and thus nothing to worry about. Indeed studies have shown that Facebook© users typically respond only to personal victimization and not second-hand knowledge of danger. Hearing of someone who has been victimized by posting personal information on Facebook© was not a strong catalyst for the use of privacy settings, it was only when they themselves experienced negative feedback that they saw the risk shift from others to themselves (Debatin*et al.* 2009).

Found to be the best predictor of risk perception and assessment, cultural theory states that individuals choose what to fear in order to support and justify their lifestyle,

having selective attention when it comes to evaluating risk. They are essentially responding to cultural understandings and deeply ingrained views of what is dangerous and what is not (Wildavsky and Dake 1990). Those who use social networking sites have a vested interest in participating in that social world and keeping up a certain image. It follows that they would not compromise that opportunity for inclusion by limiting their profile if the majority of the community has not also done so (Mesch and Beker 2010).

An important aspect of online risk unique to Facebook© and other social networking sites is the intensification of routine activities transparency. It has previously been shown that the demographics of students and their on-campus lifestyle and routine activities can create opportunities for victimization, especially for violence and theft (Fisher *et al.* 1998), and Facebook© seems to provide even more opportunity. An integral part of the Facebook© experience is the "status update," which allows users to post current thoughts and activities. It is not uncommon for users to post what they are planning on doing that day, where they will be and with whom. Another application provided by Facebook© allows users to enter their class schedule and post it directly onto their profile so others will know where they will be at exact times during the day.

This disclosure takes Routine Activities Theory to a new level, creating risk and opportunity where it has never been before. In 1979 Cohen and Felson introduced Routine Activities Theory as a criminological theory of victimization that stated, "routine activities influence criminal opportunity by bringing together offenders and victims" (Cohen and Felson 1979; Arnold, Keane and Baron 2005:346).Most criminal acts involve the meeting of motivated offenders and appropriate targets, including the absence of guardianship. Information disclosure on Facebook© could be seen as the ultimate lapse in guardianship

as users not only fail to protect their private information but voluntarily offer it to an unknown audience. If they are routinely posting their whereabouts and schedule on the site there could be ample opportunity for those looking for suitable targets to consider them as such.

There are many competing theories and reams of data on risk perception and assessment, but very little which delves into the new space of online social networking sites. These tools have created an entirely new dimension for social interaction, which has not come without consequences. The intense popularity of Facebook© among the younger generation coupled with the expectation for a high level of information disclosure has alarmed educators, advocacy groups and lawmakers into taking action to prevent further victimization (Grimmelmann 2009). Yet this action does no good if we do not understand what is prompting students to reveal so much and how (and indeed if) they are taking advantage of new privacy settings. This paper attempts to uncover if a concern for safety and the threat of possible victimization have any effect on a students' likelihood of providing private and identifiable information or using privacy settings on a publicly visible social networking site.

DATA AND METHODS

In order to investigate my hypotheses that online and physical risk perception are related to disclosure of information on Facebook, I surveyed a sample of students attending college (both graduate and undergraduate) with a series of close-ended questions indicating their perception of general risk, perception of online risk and exactly what information they disclose on Facebook©. The sample was drawn from the UNCW campus-

wide public address book that lists the names and e-mail addresses of all students and is available through the school e-mail portal. Using a random number generator, a systematic random sample was drawn, picking 3000 names from the approximately 13,000 students that currently attend UNCW. This is assumed to be a probability sample because the sampling frame from which the names were gathered is known to be complete and accurate by the college registrar. The pool that is sampled therefore has the best chance of being representative of the larger population. Those who are chosen have received an e-mail with a link to an online survey. They were given a unique link in the e-mail that will take them to the survey webpage so as to ensure that the e-mail recipient is the student taking the survey. After twelve days a follow-up e-mail was sent to students in the sample that had not responded yet. This increased the respondent rate by about 100 students.

In order to measure key concepts of the research question, students first answered a short set of demographic questions including sex, age, class year and racial/ethnic background (See Appendix for full survey). If they indicate they do not use Facebook© the online survey will proceed to the questions on physical and online risk perception, but not their information disclosure. They then filled out a 10-question assessment of personal risk concerning how at risk they feel in physical situations (as opposed to online). These included questions asking how at risk they feel walking across campus at night, leaving their belongings unattended and talking someone they do not know. Answer choices were presented in a 5-point scale ranging from "I do not feel at risk at all" to "I feel very at risk." These questions were combined for data analysis to represent perception of general risk and compared to perception of online risk and information disclosure on Facebook©.

In order to measure perceptions of online risk students answered a second set of questions similar to the first, but pertaining to online behavior. These included questions with the same scale of answers choices, asking how at risk students feel when they purchase an item online, give their name, address and phone number to a website and send e-mails. This set of questions was combined to represent perception of online risk to be compared to the other variables. Students who do not currently have a Facebook©were then asked if they have ever had one and were given an open-ended space to say why they chose to leave. The final section of questions included a chart with types of information that can possibly be disclosed on Facebook© on the vertical axis, against the groups that can possibly view it on the horizontal axis above it. Students checked only one box in each row, indicating if they list that particular data on their Facebook© page and if so, who can view it. This was followed by a final set of questions regarding use of Facebook©, which are meant to gauge the extent to which they are integrated into the Facebook© social life by asking how often they log into their account, how many friends they have and how long they have had their account (See Appendix). Questions pertaining to the use of privacy settings and potential influences on that behavior are also asked in this section, such as if family members also use the site and if they have read Facebook©'s privacy policy. These questions show the level of information disclosure and whether privacy settings are being used.

The analytical approach to this research involves comparing sets of questions that are combined to measure certain concepts, almost all of which are measured on either nominal or ordinal levels (most were then transformed to ratio-level for regression analysis). Three main concepts were measured by the survey questions: perception of

general risk, perception of online risk and level of information disclosure on Facebook©. The first two concepts are measured by a set of questions with possible response values ranging from 1-5. They were added together to produce a scale in which low values indicate less feelings of risk and high values indicate more feelings of risk. The scaled results were grouped into 3 categories of low, medium and high perception of general and online risk. The groups were analyzed against the demographic factors and other concepts in bivariate and multivariate analyses.

The analysis of the chart showing levels of disclosure on Facebook© is more complex, for there are several choices for each separate piece of information depending on the privacy settings each user has in place. The concept measured here is two-fold, looking at how much information is protected versus unprotected (open to everyone) and which pieces of information do not get posted at all. Previous research has found that women are less likely to post their address or phone number on Facebook© (Hoy & Milne 2010), which is in line with typical findings of women perceiving more potential risk than men (Franklin, Franklin & Fern 2008;Pain, 2001; Starkweather 2007; Sutton and Farral 2005).

I attempted to draw connections between perceptions of high risk in general and online and low levels of information disclosure. I expected to find that students who indicate they do not feel at risk in the physical or online world are more likely to post personal information about themselves on Facebook© and vice versa. My expectations also stem from the hypothesis that perceptions of risk online are fundamentally different than those perceived in the physical world, thus students who indicate a high level of perceived risk in general may still be willing to post more personal information on Facebook© because the two spaces are so qualitatively different. Ultimately I am looking for the

strongest predictor of the level of information disclosure on Facebook©. The factors that were analyzed as possible predictors are: perceptions of general risk, perceptions of online risk, demographics, previous victimization experience and use of Facebook© variables. I suspect that any connection between information disclosure and risk may be altered by sex, as it has been found to be a very strong predictor in relevant literature.

For the purposes of regression analysis, sex was coded as 0=female and 1=male, and class year divisions were created as dummies with seniors as the reference group. When examining the total physical risk perception score as the dependent variable with the demographic variables as independents, sex, class year (first-years and sophomores) and age were significant. Race was coded as white or non-white due to the relatively homogeneous population of UNCW.For the purposes of bivariate analysis, the age variable was condensed into three categories representing underclassmen (16 to 19), upperclassmen (20 to 22) and graduate and non-traditional students ages 23 and older.

Previous research has indicated that hiding certain parts of one's profile (such as pictures of alcohol consumption) is common and expected if a student's parents, co-workers or professors also have Facebook© and may have been able to see potentially incriminatory information (Peluchette and Karl 2010). The variable "MomhasF" indicates whether or not a student's mother (or stepmother) has a Facebook© account and they are friends with them. Thus, for each of the independent variables labeled MomhasF, DadhasF, SibhasF, RelhasF, CoworkhasF and ProfhasF, a value of 1 indicates that category of person does have Facebook© and the student is friends with them, and a value of 0 indicates they either don't have Facebook© or they aren't friends with them. The additional variables included in the regression analyses (Has your personal information been taken? Has your

FB ever been hacked? Did they join Facebook© before or after it went public? Do they have more than 500 friends) were all coded as yes=1 and no=0. All of these independent variables are also included in that analysis of who can view the most, moderately and least invasive information students post on Facebook©.

Descriptive Statistics

Of the 3,000 e-mails that were sent to the randomly chosen sample at UNCW, 646 students responded to the survey (21.5%) and 521 (17.4%) completed every question. Online surveys tend to have lower response rates, and a rate above 10% was not initially expected. The larger number of respondents was attributed to the subject matter of the survey, as Facebook© and social media are widely used among college students (Richmond 2010). The participant pool was generated randomly by the registrar's office and reflected the overall demographics of the UNCW population, as seen in Table 1, and therefore can be assumed to be representative. The largest gap in comparative demographics was in gender, where women were slightly overrepresented in the sample. The average age of respondents was 22.7, ranging from 16 to 77. Full name (70%), hometown (31%) and full birthday (27%) were the pieces of information students most often reported on Facebook© and made available for everyone (including non-friends) to see. Most photos were visible to friends only (81%), and addresses and phone numbers were the least-shared information with the majority of students not listing them on their profiles at all.

Table 1. Demographic Comparisons for Sample with UNCW Population

Demographic	Percent within UNCW	Percent within Respondents
Men	40%	27%
Women	60%	73%
Undergraduate	90%	88%
Graduate	10%	12%
White	86.5%	89%
Minority	13.5%	11%

http://uncw.edu/admissions/profile.html

RESULTS

Bivariate Analysis

The main research question deals with connecting perception of risk (both online and in physical situations), with the degree to which college students use privacy settings to protect their personal information on Facebook©. Preliminary bivariate analysis showed several interesting and expected phenomena. As age increased, the number of Facebook© friends decreased, with over 50% of those ages 16 to 19 reporting over 500 friends (See Table 2). The number of Facebook© friends one has sets the tone for how large the potential audience is that is able to gather personal information posted about the user. Indeed it was found that younger Facebook© users (those with more friends) were significantly more likely to post photos that indicated where they lived and to have more Facebook© friends that they weren't acquainted with in real life. Over 75% of students ages 16 to 19 reported having Facebook© friends they hadn't actually met in person and were most likely to post photos identifying their residence. In contrast, over half of those 23 and older did not have any unknown friends or pictures of their residence on Facebook©.

On the surface, this would suggest that younger students are less concerned with Facebook© privacy and guarding their personal information online, but when asked directly about the level of importance of Facebook© privacy, there was no significant relationship between the age groups. Over 70% of students reported that Facebook© privacy was important to them regardless of age (See Table 2). This is one of the disconnects I expected to find based on previous research that younger college students report the same level of concern for online privacy yet are less willing to withhold information in favor of taking advantage of social networking (Starkweather 2007). Several questions aimed at gauging the influence of personal experience with identity theft showed that younger students were slightly more likely than older students to have experienced someone hacking into their Facebook© account, yet older students were more likely to have had their other personal information stolen and used without their consent (See Table 2). This may provide some insight into why older students would be more likely to protect their information on Facebook©.

Sex was a significant predictor of the reported level of privacy importance, and the number of unknown friends (with females being more likely to consider privacy important and to have less unknown friends), yet it did not play a role in how many total Facebook© friends one had or their experience with identity theft or Facebook© hacking (See Table 3). Surprisingly, there was no correlation between gender and the number of photos one had that identified their residence, yet 90% of females and 81% of males did not list their current address on their profiles. Although photos posted of self was significant in Table 3, it is clear that the chi-square was artificially inflated due to the very small number of students overall who said they did not post photos.

Table 2. Descriptive Statistics for Variables in the Bivariate Analyses by Age

Variable	16-19 Column Percent	20-22 Column Percent	23 and older Column Percent	Chi-Sq.
500 or more Friends	51.3	49.5	18.4	84.161*
FB Privacy Important	75.3	77.6	71.8	9.103
Has Unknown Friends	77.8	65.6	48.6	37.880*
Has Photos of Residence	65.2	56.1	42.6	28.673*
Had/DK Identity Stolen	33.9	30.5	36.1	15.818*
Had Facebook Hacked	14.0	14.3	12.1	7.092
FB Indicates Schedule	34.8	33.8	26.8	11.861*
Never Read Priv. Policy	50.0	52.9	48.2	9.689
Lists Full Name	95.6	94.6	92.3	18.532*
Lists Full Birthdate	76.9	72.5	64.5	6.928
Lists Current Address	14.1	9.9	14.3	2.915
Lists E-mail Address	64.7	73.9	64.3	5.172
Lists Current Phone #	36.3	28.3	29.5	3.372
Lists Hometown	88.0	87.4	86.4	.207
Lists Job	59.9	61.7	70.0	5.839
Posts Photos of Self	100	98.7	98.6	4.758
Lists IM Screen Name	25.6	29.1	36.0	4.054

* = Significant at .05.

Table 3. Descriptive Statistics for Variables in the Bivariate Analyses by Sex

	Men	Women	
Variable	Column Percent	Column Percent	Chi-Sq.
500 or more Friends	49.6	48.0	4.201
FB Privacy Important	58.9	80.7	42.906*
Has Unknown Friends	69.5	63.2	8.159*
Has Photos of Residence	53.5	55.8	1.704
Had/DK Identity Stolen	39.9	31.0	5.414
Had Facebook Hacked	15.6	12.9	1.009
FB Indicates Schedule	24.2	34.7	5.130
Never Read Priv. Policy	65.9	45.9	18.534*
Lists Full Name	95.3	93.9	2.980
Lists Full Birthdate	79.0	69.3	10.857*
Lists Current Address	19.5	10.0	16.674*
Lists E-mail Address	65.9	69.2	1.159
Lists Current Phone #	41.7	27.5	30.9976*
Lists Hometown	90.6	86.3	2.915
Lists Job	68.8	61.5	5.803
Posts Photos of Self	99.2	99.0	10.472*
Lists IM Screen Name	34.1	28.5	1.999

* Significant at .05.

OLS Regression Analysis

As Table 4 shows, females and older students were significantly more likely to have a higher score on the physical risk perception scale, while, in comparison to seniors, first-year students and sophomores were significantly more likely to have a lower physical risk perception score. The adjusted R square for this analysis was .097, indicating that only about 10% of the variation in the physical risk perception score was accounted for by these demographic variables. Race was not significantly associated with the physical risk perception score.When examining the total online risk perception score as the dependent variable, the total physical risk perception score was included with the demographic variables as an independent variable. This is because socialization and formation of physical risk would logically develop before one learns to use the Internet, thus possibly carrying over some of the same logic. Indeed physical risk perception did prove to be significantly correlated with online risk perception, as did sex (See Model 1, Table 4). Females and those who perceive a higher physical risk were more likely to perceive a higher online risk as well. However the R square value for this analysis was .062, indicating that only about 6% of the variation in the total online risk perception score was explained by these variables.

However, when two additional variables were added as controls, we see these numbers shift considerably (See Model 2, Table 4). The questions of "Have you ever had your personal information taken?" and "Has your Facebook© account ever been hacked?" could logically influence online risk perception scores if previous experience has taught students to be more cautious on the internet and with their personal information. When these independent variables were added with the previous demographic variables and the

physical risk perception score, the relationship between online risk and sex is no longer significant. Rather, physical risk perception emerges as the only significantly correlated factor to online risk perception scores. The adjusted R square value for this analysis is 0.051, indicating that it is slightly less predictive than the previous analysis.

Table 4. Beta Values for Risk Perception Scales

DV	Physical Risk Perception Score	Online Risk Perception Score Model 1	Online Risk Perception Score Model 2
Adjusted R-square	.097	.062	.051
IV			
Sex	-.189***	-.090*	-.083
Age	.143**	.070	.075
White or Non-White	.032	.001	.006
First-years	-.131**	.000	.013
Sophomores	-.105*	.066	.076
Juniors	-.025	-.036	-.032
Grad Students	.064	-.023	-.034
Physical Risk Score	-	.220***	.212***
Personal Info Taken[1]	-	-	-.034
Facebook Hacked[2]	-	-	.009

*= Significant at .05 **=Significant at .01 ***=Significant at .001

The principle purpose of determining students' perception of online and physical risk was to compare those scores against the use of Facebook© privacy settings and what information they were willing to divulge in a public forum. Use of Facebook©'s privacy settings were measured by questions indicating what information students had posted on

[1] "Has your personal information ever been taken?" Coded as Yes=1 No=0

[2] "Has your Facebook ever been hacked?" Coded as Yes=1 No=0

their profile, and to whom these elements were visible. Level of visibility (ranging from 'everyone' to 'not listed on profile'), of the nine profile aspects was analyzed in factor analysis to in order to combine these variables into meaningful categories. Factor analysis revealed a distinct pattern among these nine questions(See Table 5), which was then used to combine the nine variables into three dependent variables measuring privacy settings in relation to most, moderately and least invasive information.

Table 5. Factor Analysis for Level of Information Disclosure Questions

Rotated Component Matrix	Component		
	1	2	3
Who is your phone number visible to on Facebook?	.687	.263	.098
Who is your address visible to on Facebook?	.677	.092	-.086
Who is your IM screen name visible to on Facebook?	.662	.098	.088
Who is your e-mail address visible to on Facebook?	.616	-.027	.327
Who is your job visible to on Facebook?	.265	.721	-.037
Who is your hometown visible to on Facebook?	.040	.673	.369
Who are your photos visible to on Facebook?	.055	.644	.060
Who is your full name visible to on Facebook?	.044	.000	.869
Who is your full birthdate visible to on Facebook?	.173	.309	.634

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

The variable which combines the least invasive information (full name and full birthday) was analyzed as the dependent variable with the following independent variables: sex, class year dummy variables, age, race (as white or non-white), total physical risk perception score, total online risk perception score, whether they joined Facebook© before or after it was open to all users, how often they access Facebook©, how many friends they have, when they last read Facebook©'s privacy policy, if their personal information

was ever taken, if their Facebook© account had ever been hacked and how important Facebook© privacy is to them. In addition, six variables were computed using the "check all that apply" questions pertaining to who else in the students' lives have Facebook© accounts and if they are friends with them.

Table 6 shows the t-ratios, standardized beta coefficients and significance for independent variables analyzed with the factor analysis scores of the "least invasive information" dependent variable. This analysis showed that younger students, those of the junior class, those who had a higher online risk perception score and those who were friends with their professors on Facebook© were significantly more likely to have restricted visibility to their full name and full birthdate on Facebook© (or less likely to have it visible to more people). Using the same set of independent variables, Tables 7 and 8 show results for the factor analysis scores of moderately invasive and most invasive information. For the moderately invasive information (photos, hometown and job), men, those who were friends with their co-workers and those with more than 500 friends were significantly more likely to share their photos, hometown and job with more people on Facebook©. Joining Facebook© before it was publicly available to join was only independent variable in this set that decreased the likelihood of sharing this information. In Table 8 we see that men and those with more than 500 friends are significantly more likely to have their most invasive personal information (phone number, address, e-mail address and instant message screen name) visible to more people. Students with a higher online risk perception score were more likely to protect this information and restrict the access other Facebook© users had to it.

Table 6. Results for Least Invasive Information

Model 1 Dependent Variable: Factor Analysis Score for Least Invasive Information N=498 R Square=. 103 Adjusted R Square=. 067	t-ratios	Standardized Beta Coefficients
Sex	.635	.029
Age	**-2.092**	**-.113***
White or non-white	.885	.040
First-year Students	-.544	-.031
Sophomore Students	.037	.002
Junior Students	**-2.230**	**-.122***
Graduate Student	-1.621	-.088
Total Physical Risk Perception Score	-.605	-.028
Total Online Risk Perception Score	**-3.201**	**-.145*****
Mom has FB and they are friends with her	-.577	-.027
Dad has FB and they are friends with them	1.747	.084
Sibling(s) has FB and they are friends with them	1.189	.054
Other relative(s) has FB and they are friends with them	.721	.034
Co-workers have FB and they are friends with them	-.329	-.015
Profs have FB and they are friends with them	**-1.985**	**-.090***
Personal Information has been taken (Yes=1)	.066	.003
Facebook has been hacked (Yes=1)	-.842	-.037
Joined Facebook after it went public (Yes=1)	-.769	-.038
More than 500 friends (Yes=1)	.050	.002

* = Significant at .05 ** = Significant at .01 *** = Significant at .001

Table 7. Results for Moderately Invasive Information

Model 2 Dependent variable: Factor Analysis Score for Moderately Invasive Information N=498 R Square= .118 Adjusted R Square= .083	t-ratios	Standardized Beta Coefficients
Sex	**2.200**	**.098***
Age	1.938	.104
White or non-white	-.197	-.009
First-year Students	1.816	.103
Sophomore Students	1.191	.066
Junior Students	1.217	.066
Graduate Student	1.822	.098
Total Physical Risk Perception Score	-1.711	-.080
Total Online Risk Perception Score	-1.944	-.088
Mom has FB and they are friends with her	.431	.020
Dad has FB and they are friends with them	.704	.033
Sibling(s) has FB and they are friends with them	-1.472	-.066
Other relative(s) has FB and they are friends with them	-.360	-.017
Co-workers have FB and they are friends with them	**4.078**	**.186*****
Profs have FB and they are friends with them	1.523	.068
Personal Information has been taken (Yes=1)	-.410	-.018
Facebook has been hacked (Yes=1)	.714	.032
Joined Facebook after it went public (Yes=1)	**-2.369**	**-.117***
More than 500 friends (Yes=1)	**2.703**	**.119****

* = Significant at .05 ** = Significant at .01 *** = Significant at .001

Table 8. Results for Most Invasive Information

Model 3 Dependent variable: Factor Analysis Score for Most Invasive Information N= 498 R Square= .080 Adjusted R Square= .043	t-ratios	Standardized Beta Coefficients
Sex	**3.007**	**.137****
Age	.408	.022
White or non-white	-.664	-.030
First-year Students	-.219	-.013
Sophomore Students	1.236	.070
Junior Students	1.037	.057
Graduate Student	-1.266	-.070
Total Physical Risk Perception Score	1.331	.063
Total Online Risk Perception Score	**-2.343**	**-.108***
Mom has FB and they are friends with her	.982	.047
Dad has FB and they are friends with them	.947	.046
Sibling(s) has FB and they are friends with them	.756	.035
Other relative(s) has FB and they are friends with them	.461	.022
Co-workers have FB and they are friends with them	.413	.019
Profs have FB and they are friends with them	1.092	.050
Personal Information has been taken (Yes=1)	1.223	.056
Facebook has been hacked (Yes=1)	-1.356	-.061
Joined Facebook after it went public (Yes=1)	1.399	.070
More than 500 friends (Yes=1)	**2.152**	**.097***

* = Significant at .05 ** = Significant at .01 *** = Significant at .001

Binary Logistic Regression Analysis

Two additional variables were analyzed using binary logistic regression due to the categorical nature of their responses. "Do you have any friends that you do not know in real life?" and "Do you have any photos posted that identify where you live?" were collapsed into yes=1 and no=0. These questions measure information protection on another level that the previous questions did not. If a student is allowing their profile to be fully accessed

to “friends” that are actually unknown to them, the practice of limiting certain information to “friends only” may not be as effective at protecting privacy. Likewise with pictures of their residence, this makes it much easier for strangers and even “friends” to find them and could theoretically increase their likelihood of victimization. These variables were analyzed with the same set of independent variables, as were the previous sets of dependent variables in the OLS regression analysis. Table 9 shows standard error, beta values and significance for Model 4 (unknown friends) and Table 10 shows the same information for Model 5 (residence ID photos).

For the likelihood of having unknown Facebook© friends, a student’s age and total online risk perception score were significantly correlated with a decreased probability of having such friends. Thus older students and those with a higher online risk perception score were less likely to have any friends on Facebook© that they did not actually know in real life. For each additional year of age, the odds of having unknown Facebook© friends decrease by 5.4%. This echoes the bivariate analysis done which showed that as student age increased, the percentage of those with unknown friends decreased. For each unit increase in the total online risk perception score, the odds of having an unknown Facebook© friend decrease by 2.4%. Being a part of the junior class significantly increased the likelihood of having friends who were not actually known, with juniors being 6.4% more likely to have unknown friends. The Block 0 percentage for this model was 64.3%, and the Block 1 percentage increased to 68.8% after the independent variables were taken into account.

For the odds of students having photos on their Facebook© that identify their residence, first-year students and those with more than 500 friends were significantly

more likely to post such pictures than seniors and those with less than 500 friends. Freshmen students were more than twice as likely as those of other classes to have pictures of where they live, and students with more than 500 friends were 57% more likely to post pictures identifying their residences. The Block 0 percentage for this model was 55.3%, and the Block 1 percentage increased to 61.5% after the independent variables were taken into account.

Table 9. Students with Unknown Friends

Model 4 Dependent Variable: Does student have unknown friends? N=512	Standardized Coefficients		Exp(B)
	Beta	Std. Error	
Sex	.342	.241	1.408
Age	**-.052****	**.020**	**.949****
White or non-white	-.024	.324	.976
First-year Students	.673	.361	1.960
Sophomore Students	.110	.305	1.117
Junior Students	**.062***	**.283**	**1.064***
Graduate Student	-.610	.357	.543
Total Physical Risk Perception Score	.005	.011	1.005
Total Online Risk Perception Score	**-.024****	**.008**	**.977****
Mom has FB and they are friends with her	-.023	.217	.977
Dad has FB and they are friends with them	-.246	.217	.782
Sibling(s) has FB and they are friends with them	-.150	.288	.860
Other relative(s) has FB and they are friends with them	.326	.366	1.385
Co-workers have FB and they are friends with them	.291	.226	1.338
Profs have FB and they are friends with them	-.239	.240	.787
Personal Information has been taken (Yes=1)	.134	.316	1.144
Facebook has been hacked (Yes=1)	.152	.295	1.164
Joined Facebook after it went public (Yes=1)	.122	.302	1.130
More than 500 friends (Yes=1)	.250	.199	1.284

*=Significant at .05 ** = Significant at .01 *** = Significant at .001

Table 10. Photos Identifying Residence

Model 5 Dependent Variable: Does student have photos identifying their residence? N=514	Standardized Coefficients		Exp(B)
	Beta	Std. Error	
Sex	-.100	.223	.905
Age	-.027	.019	.974
White or non-white	.293	.305	1.341
First-year Students	**.701***	**.328**	**2.015***
Sophomore Students	.467	.294	1.595
Junior Students	-.021	.267	.979
Graduate Student	-.347	.352	.707
Total Physical Risk Perception Score	.005	.010	1.005
Total Online Risk Perception Score	.002	.008	1.002
Mom has FB and they are friends with her	.269	.205	1.309
Dad has FB and they are friends with them	-.019	.206	.981
Sibling(s) has FB and they are friends with them	.017	.272	1.017
Other relative(s) has FB and they are friends with them	-.655	.365	.519
Co-workers have FB and they are friends with them	.130	.216	1.139
Profs have FB and they are friends with them	-.335	.232	.715
Personal Information has been taken (Yes=1)	.448	.305	1.565
Facebook has been hacked (Yes=1)	-.131	.274	.877
Joined Facebook after it went public (Yes=1)	.070	.291	1.072
More than 500 friends	**.451***	**.189**	**1.571***

* = Significant at .05 ** = Significant at .01 *** = Significant at .001

Qualitative Data

Included in the questionnaire was an option for students who do not currently have an active Facebook© account but did at one point and chose to close it. While they were not prompted to answer the questions pertaining to level of visibility of their information, there was an open-ended question providing room to explain why they chose to leave Facebook©. Twenty-seven students chose this option and relayed quite candid explanations as to why they no longer use Facebook©. The greatest concern mentioned by 14 out of 27 respondents was that Facebook© became too invasive and they were uncomfortable with the lack of privacy. One student wrote, "The fact that other people could post pictures of me or communicate what I was doing without my permission and all their friends could see/know even though I had a very private/restricted account." This suggests that although Facebook© has recently provided more options for privacy settings, some students still find them inadequate to protect their information at a level that they would feel comfortable using the site. Some went as far to say that it was an "acceptable form of stalking," and they felt the information they were pressured to provide was too personal. A few students pointed out the ignorance of others by sarcastically stating, "People decide it's smart to post a minute my minute description of what they are doing." Somewhat surprising was the fact that men were more likely to cite privacy concerns as a reason for leaving Facebook© than were women. Clearly this group is recognizing the risk users put themselves at by posting such information, but it is doubtful that those who chose to delete their profiles are the only ones who realize this danger.

The second most-cited reason for leaving Facebook© (mentioned by 11 out of 27 respondents) was the sheer amount of time it was consuming from their lives. Several

students referenced the addictive quality of Facebook© and recognized that they fell into a "trap" of relying on it too much for communication and entertainment. There was an interesting, although not surprising, perception that many students spend vast amounts of time on the site. One student commented "I didn't want to spend hours on it like everyone else does." Here we see the perception of its importance to staying connected to the college social scene and the assumption of use by users and non-users alike. Others found themselves "wasting my own free time," and coming to the conclusion that it was a "colossal waste of time."

A female junior pensively wrote about the society Facebook© creates online and how that translates into different behavior offline. "It turns people into people they are not. Most people wouldn't actually stalk other people in real life, but they do it behind the safety of the screen. I also don't like how people are consumed by it and they live by the Facebook© rules." This comment gets at the concept of an online community creating and policing it's own rules and standards of conduct and just how powerful these expectations can be. A young lady made the point of saying, "My family put too much pressure on me to put stuff on it or take stuff off of it." This relates directly to the questions asked later in the survey for current Facebook© users (Were they friends with their parents/co-workers/professors etc. on Facebook©?). Part of the rules of the Facebook© community that can be found nowhere in written form but somehow are passed down through socialization of the network itself, include the assumption that students will hide certain behavior from their parents and other authority figures. This gives the impression that they realize what they are doing and posting about is inappropriate and not something they

would feel comfortable sharing with their parents, but yet they are still willing to make those images available for hundreds of peers to see.

Personal issues and bad experiences with Facebook© were also a common thread amongst students who had decided to leave. A male student wrote of the pain of a break-up and not wanting to see his ex-girlfriend's new activities. Several students wrote (rather humorously) of the inane purpose of social networking in general, a male senior stated, " If I wanted to keep in touch with my dog's trainer's mother's sister's uncle, then I would've a long time ago." Many expressed a distain for the constant and targeted advertising and the sale of their information to marketers, while others were starting to be concerned that the information on their profile might make it difficult to get a job if a potential employer decided to look them up. One final student (a male sophomore) summed it up rather eloquently by saying that Facebook© was like, "being constantly connected without much real connection." Overall these responses were encouraging and show that students are aware of the risks of social media and full disclosure to such a wide and unknown audience. Those who recognize the value of actual interaction and privacy may be taking a step in the right direction to helping the rest of their peers better monitor their safety and information.

CONCLUSIONS AND DISCUSSION

Based on this research study, the hypothesis stating that an online perception of risk negatively influences information college students post on Facebook© was mostly supported. The data found that a higher score on the online risk perception scale lead to a lower likelihood of making one's full name, full birthdate, phone number, address, instant

message screen name and e-mail address visible to more people on Facebook©. The fact that scores from the physical risk perception scale were not directly significant in any of the analyses supports my original hypothesis that perceptions of risk differ from the online world to the physical one. However, physical risk perception was a significant prediction of online risk perception, which was significant in the analyses. In this case, it may be that different cues and expected community standards are used to assess online situations and may result in students behaving differently when it comes to giving out their personal information. Online risk perception score was also found to be a negative predictor of whether or not students had Facebook© friends that they did not know in real life. This suggests that students are at least somewhat aware of the dangers that online activity can pose when making personal knowledge available to unknown persons.

Sex played less of a role than was expected, perhaps because of the high degree of correlation between sex and the risk scales (with females being significantly more likely to score higher on both risk scales). However, this was not true when previous experience with Facebook© hacking and information theft was taken into account (See Figure 1). Male students were significantly more likely to have their most invasive information (address, phone number, e-mail and instant message screen name) as well as their moderately invasive information (hometown and job) visible to more people on Facebook.© Age was negatively correlated with having friends who were not known in person, and as age and class year increased, it became less likely students would befriend unknown persons and more likely they would have less Facebook© friends overall. First-year students were shown to have the greatest number of friends on average, which was also correlated with having photos posted that identified their residence. Having discussed this phenomenon

with several classes of undergraduate students, the consensus was that first-year students may be more eager to try to fit in and make friends in a new place and would sacrifice privacy for increased social exposure.

Limitations and Future Research

Although this was a somewhat long and complex study with questions covering many aspects of the Facebook© social life, there are still many questions left unanswered when it comes to how students make the decision to post certain information on their profile. The questions pertaining to friendships with authority figures and different types of audiences did not have the influence I had predicted. Over 50% of students were friends with their mother (or stepmother) on Facebook©, over 40% were friends with their father (or stepfather) and over 20% were friends with their professors, yet this did not significantly impact their likelihood of sharing any aspects of personal information with a greater number of people on Facebook©. If this study were to be repeated, more questions tailored towards how and why students make choices to post specific information on their profiles would be useful in a examining this topic.

Limitations include sample size and the homogeneous nature of this particular campus population. Questions about social class background were not asked due to initial assumptions that it was unrelated, but could be asked in future research to see how social class influences how students learn to interpret physical and online risks. It is clear from this research that there is a disconnect between what students claim to believe about online privacy and what they actually do on the Internet. Now that Facebook© is open to

anyone ages 13 and above, it will be critical that parents and educators start early with teaching kids about the potential consequences of posting personal information online.

REFERENCES

Arnold, Robert, Keane, Carl and Stephen Baron. 2005. "Assessing Risk of Victimization through Epidemiological Concepts: An Alternative Analytic Strategy Applied to Routine Activities Theory." *The Canadian Review of Sociology and Anthropology* 42(3): 345-363.

Boyd, Danah and EszterHargittai. 2010. "Facebook© privacy settings: Who cares?" *First Monday* 15(8). August 2.

Bureau of Justice Statistics. 2006. Victimization Rates for Persons Age 12 and Over. http://www.ojp.usdoj.gov/bjs.

Chadee, Derek, Liz Austen and Jason Ditton. 2007. "The Relationship Between the Likelihood and Fear of Criminal Victimization." *The British Journal of Criminology* 47(1):133-153.

Christofides, Emily, Amy Muise and Serge Desmarais. 2009. "Information Disclosure and Control on Facebook©: Are They Two Sides of the Same Coin or Two Different Processes?" *CyberPsychology& Behavior* 12(3): 341-345.

Cohen, L.E. and M. Felson (1979). "Social Change and Crime Rate Trends: A Routine Activity Approach." American Sociological Review 44:588-608.

CyberTipline. "Think Before You Post: Social Networking Sites." National Center for Missing and Exploited Children.Accessed October 1, 2010.

Debatin, Bernhard, Lovejoy, Jennette P., Horn, Ann-Kathrin and Brittany N. Hughes. 2009. "Facebook© and Online Privacy: Attitudes, Behaviors and Unintended Consequences." *Journal of Computer Mediated Communication* 15:83-108.

Ditton, Jason and Derek Chadee. 2005. "People's Perception of Their Likely Future Risk of Criminal Victimization." *British Journal of Criminology* 46:505-518.

Ferraro, Kenneth F. 1995. Fear of Crime: Interpreting Victimization Risks. Albany, NY : SUNY Press.

Fisher, Bonnie S., Sloan, John T., Cullen, Francis T. and Chunmeng Lu. 1998. "Crime in the Ivory Tower: The Level and Sources of Student Victimization." *Criminology* 36(3): 671-710.

Franklin, Travis W., Cortney Franklin and Noelle E. Fearn. 2008. "A Multilevel Analysis of the Vulnerability, Disorder and Social Integration Models of Fear of Crime." *Social Justice Review* 21:204-227.

Goffman, Erving. 1959. *The Presentation of Self in Everyday Life*. First Anchor Books Edition. Random House Inc, New York.

Grimmelmann, James. 2009. "Saving Facebook©." *University of Iowa Law Review* 94:1137-1216.

Hoadley, Christopher M., Xu, Heng, Lee, Joey J., and Mary Beth Rosson. 2010. "Privacy as information access and illusory control: The case of the Face book News Feed privacy outcry." *Electronic Commerce Research and Applications* 9:50-60.

Hoy, Mariea Grubbs and George Milne. 2010. "Gender Differences in Privacy-Related Measures for Young Adult Facebook Users." *Journal of Interactive Advertising* 10(2): 28-45.

Ibrahim, Yasmin. 2008. "The new risk communities: Social networking sites and risk." *International Journal of Media and Cultural Politics* 4(2): 245-253.

Kite, Stacey L., Gable, Robert and Lawrence Filippelli. 2010. "Assessing Middle School Students' Knowledge of Conduct and Consequences and Their Behaviors Regarding the Use of Social Networking Sites." *The Clearing House* 83:158-163.

Lane, Jodi, Gover, Angela R. and Sara Dahod. 2009. "Fear of Violent Crime Among Men and Women on Campus: The Impact of Perceived Risk and Fear of Sexual Assault." *Violence and Victims* 24(2): 172-192.

Lewis, Kevin, Jason Kaufman and Nicholas Christakis. 2008. "The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network." *Journal of Computer-Mediated Communication* 14:79-100.

Livingstone, Sonia. 2008. "Taking risky opportunities in youthful content creation: teenagers ' use of social networking sites for intimacy, privacy and self-expression." *New Media & Society* 10(3): 393-411.

Mead, George Herbert. 1967. *Mind, Self and Society: From the Standpoint of a Social Behavioralist.*University of Chicago Press.

Melde, Chris. 2009. "Lifestyle, Rational Choice, and Adolescent Fear: A Test of a Risk-Assessment Framework." *Criminology* 47(3): 781-812.

Mesch, Gustavo S. 2000. "Perceptions of risk, lifestyle activities, and fear of crime."*Deviant Behavior* 21:47-62.

Mesch, Gustavo S. and Guy Beker. 2010. "Are Norms of Disclosure of Online and Offline Personal Information Associated with Disclosure of Personal Information Online?" *Human Communication Research* 36:570-592.

Pain, Rachel. 2001. "Gender, Race, Age and Fear in the City." *Urban Studies* 38:899-913.

Peluchette, Joy and Katherine Karl. 2010. "Examining Students' Intended Image on Facebook©: "What Were They Thinking?!" *Journal of Education for Business* 85:30-37.

Reid, Lesley Williams and Miriam Konrad. 2004. "The Gender Gap in Fear: Assessing the Interactive Effects of Gender and Perceived Risk on Fear of Crime." *Sociological Spectrum* 24:399-425.

Richmond, Riva. 2010. "A Guide to Facebook©'s New Privacy Settings." *The New York Times* May 27. Accessed September 26, 2010.

Rippl, Susanne. 2002. "Cultural theory and risk perception: a proposal for a better measurement." *Journal of Risk Research* 5(2): 147-165.

Seale, Clive. (2007). *Researching Society and Culture: Second Edition*. London: Sage Publications.

Smith, William R. and Marie Tortensson. 1997. "Gender Differences in Risk Perception and Neutralizing Fear of Crime." *British Journal of Criminology* 37 (4): 608-634.

Starkweather, Sarah. 2007. "Gender, Perceptions of Safety and Strategic Responses among Ohio University Students." *Gender, Place and Culture* 14(3):355-370.

Sutton, Robbie M. and Stephen Farral. 2005. "Gender, Socially Desirable Responding and the Fear of Crime: Are women really more anxious about crime?" *The British Journal of Criminology* 45(2):212-214.

Taraszow, Tatjana, Elena Aristodemou, Georgina Shitta, YiannisLaouris and AsyuArsoy. 2010. "Disclose of personal and contact information by young people in social networking sites: An analysis using Facebook© profiles as an example." *International Journal of Media and Cultural Politics* 6(1): 81-102.

Thacker, Matt. 2010. "New Albany woman claims Facebook© 'friend' burglarized home." *News and Tribune* March 23. Accessed September 26, 2010.

Timm, Dianne M. and Carolyn J. Duven. 2008. "Privacy and Social Networking Sites." *New Directions for Student Services* Winter 124: 89-102.

Tufekci, Zeynep. 2008. "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites."*Bulletin of Science and Technology* 28(1): 20-36.

vanManen, Max. 2010. "The Pedagogy of Momus Technologies: Facebook©, Privacy, and Online Intimacy." *Qualitative Health Research*20(8): 1023-1032.

Wilcox, Pamela., Carol E. Jordan and Adam J. Pritchard. 2007. "A Multidimensional Examination of Campus Safety: Victimization, Perceptions of Danger, Worry about Crime and Precautionary Behavior Among College Women in the Post-Clery Era." *Crime and Delinquency* 53(2):219-254.

Wildavsky, Aaron and Karl Dake. 1990. "Theories of Risk Perception: Who Fears What and Why?" *Journal of the American Academy of Arts and Sciences* 119(4): 41-60.

Winterdyk, John and Nikki Thompson. 2008. "Student and Non-Student Perceptions and Awareness of Identity Theft." *Canadian Journal of Criminology and Criminal Justice* April 2008:153-186.

Appendix

Thank you for agreeing to participate in this survey. This survey is geared towards understanding students' use of the social networking site, Facebook. Remember that participation in this survey is completely voluntary, so if there are any questions you don't wish to answer, just leave them blank. All your responses will be kept strictly confidential; your answers will be analyzed only in statistical summaries with other respondents, and therefore will not be individually identifiable. Most of the questions ask you to mark the response that most closely describes your experiences or opinion, although some ask you to type your answer in the box provided. Please give only one answer to each question, unless otherwise instructed.

1. What is your sex?
   - [ ] Male
   - [ ] Female

2. What is your current class year at UNCW?
   - [ ] First-year
   - [ ] Sophomore
   - [ ] Junior
   - [ ] Senior
   - [ ] Graduate Student

3. What is your racial/ethnic background?
   - [ ] Asian
   - [ ] Black (non-Hispanic)
   - [ ] White (non-Hispanic)
   - [ ] Latino
   - [ ] Multiracial

4. What is your age? _____

Perception of General Risk

5. For each of the following questions, please indicate on a 1-5 scale to what degree you feel at risk for criminal victimization during the listed activities, with a score of "1" indicating that you feel no risk at all, and a score of "5" indicating you feel very at risk. If an activity does not apply to you then please select "N/A."

N/A	**1**	**2**	**3**	**4**	**5**	**Walking alone around central parts of campus during the day**
N/A	**1**	**2**	**3**	**4**	**5**	**Walking alone to your residence during the day**
N/A	**1**	**2**	**3**	**4**	**5**	**Walking alone around central parts of campus at night**
N/A	**1**	**2**	**3**	**4**	**5**	**Walking alone to your residence at night**
N/A	**1**	**2**	**3**	**4**	**5**	**Leaving belongings unattended at the library**
N/A	**1**	**2**	**3**	**4**	**5**	**Walking around off campus with friends at night**
N/A	**1**	**2**	**3**	**4**	**5**	**Walking around off campus alone at night**

N/A	**1**	**2**	**3**	**4**	**5**	**Leaving a bike unlocked on campus**
N/A	**1**	**2**	**3**	**4**	**5**	**Talking to someone you do not know on campus**
N/A	**1**	**2**	**3**	**4**	**5**	**Talking to someone you do not know off campus**

Perception of Online Risk

6. For each of the following questions, please indicate on a 1-5 scale to what degree you feel at risk for criminal victimization during the listed activities, with a score of "1" indicating that you feel no risk at all, and a score of "5" indicating you feel very at risk.If an activity does not apply to you then please select "N/A."

N/A	**1**	**2**	**3**	**4**	**5**	**Purchasing an item online using a credit card**
N/A	**1**	**2**	**3**	**4**	**5**	**Giving your social security number to a financial aid website**
N/A	**1**	**2**	**3**	**4**	**5**	**Providing bank account numbers for online tuition refunds**
N/A	**1**	**2**	**3**	**4**	**5**	**Posting pictures of yourself on websites**
N/A	**1**	**2**	**3**	**4**	**5**	**Sending an e-mail using the UNCW mail server**
N/A	**1**	**2**	**3**	**4**	**5**	**Visiting websites while using the UNCW internet network**
N/A	**1**	**2**	**3**	**4**	**5**	**Entering your name, address or phone number in a website**
N/A	**1**	**2**	**3**	**4**	**5**	**Using an Instant Messenger program to talk to a friend**
N/A	**1**	**2**	**3**	**4**	**5**	**Using a live video-chat program**
N/A	**1**	**2**	**3**	**4**	**5**	**Communicating with someone online you do not know**

7. Do you currently have an active Facebook account?

[ ] Yes (If yes, direct to question 10)
[ ] No (If no, direct to question 8)

8. Have you ever had a Facebook account?

[ ] Yes
[ ] No (If no, end survey)

9. If you have had a Facebook account in the past but currently do not, please give a brief explanation as to why you decided to leave Facebook

10. The following chart lists types of information that you can post on Facebook and whom it is visible by. Please check the appropriate box as it applies to the information posted on your Facebook profile and who can see it.

	Everyone	Only UNCW Network	Friends Only	Only Certain Friends	Not Listed on Profile
Full name*					
Full Birthday*					
Address/Dorm					
E-mail					
Phone Number					
Hometown					
Job					
Photos					
IM screen name					

* Full name refers to first and last name
* Full birthday refers to date, month and year

11. When did you first create your Facebook account?
- [ ] When I was in high school
- [ ] Between high school and college
- [ ] When I first came to college
- [ ] After I had been in college

12. How often do you access Facebook?
- [ ] More than 5 times per day
- [ ] 1-5 times per day
- [ ] Less than once per day
- [ ] Less than once per week
- [ ] Less than once per month

13. Is your profile publicly searchable on search engines?
- [ ] Yes
- [ ] No
- [ ] Don't know

14. Approximately how many friends do you currently have on Facebook?
- [ ] Under 100
- [ ] 100-300
- [ ] 300-500
- [ ] 500-700
- [ ] Over 700

15. Do you have friends on Facebook that you do not know in person?

[ ] Yes, I have more than 10
[ ] Yes, I have between 3 and 10
[ ] Yes, I have one or two
[ ] No, I do not have any

16. Which of the following people you know also have a Facebook profile? Please check all that apply

[ ] My mother
[ ] My father
[ ] My sibling(s)
[ ] Other relatives
[ ] Co-workers
[ ] Professors

17. Of the previous answers, which of the following are you friends with on Facebook? Please check all that apply

[ ] My mother
[ ] My father
[ ] My sibling(s)
[ ] Other relatives
[ ] Co-workers
[ ] Professors

18. When was the last time you read Facebook's privacy policy?

[ ] In the last month
[ ] In the last 3 months
[ ] In the last 6 months
[ ] In the last year
[ ] I have never read Facebook's privacy policy

19. Do you have pictures posted (and tagged) of you on Facebook that identify where you live?

[ ] Yes, I have more than 10
[ ] Yes, I have between 3 and 10
[ ] Yes, I have one or two
[ ] No, I do not have any

20. Do you post any information on your Facebook profile (such as status updates, etc.) that indicates your daily activities or schedule?

[ ] Yes
[ ] No