

Rochester Institute of Technology

RIT Digital Institutional Repository

Theses

1-1-2006

The phenomenon of cyberstalking on the RIT campus: Definitions, behaviors and normalization

Julia Phillips Dickinson

Follow this and additional works at: <https://repository.rit.edu/theses>

Recommended Citation

Dickinson, Julia Phillips, "The phenomenon of cyberstalking on the RIT campus: Definitions, behaviors and normalization" (2006). Thesis. Rochester Institute of Technology. Accessed from

This Thesis is brought to you for free and open access by the RIT Libraries. For more information, please contact repository@rit.edu.

Running head: PHENOMENON OF CYBERSTALKING

The Phenomenon of Cyberstalking on the RIT Campus:
Definitions, Behaviors and Normalization

A Thesis Presented to The Faculty of the Department of Communication
Rochester Institute of Technology

In Partial Fulfillment of the Master of Science Degree in
Communication & Media Technologies

by

Julia Phillips Dickinson

August 14, 2006

Thesis/Dissertation Author Permission Statement

Title of thesis or dissertation:

The Phenomenon of Cyberstalking on the RIT Campus: Definitions, Behaviors and Normalization

Name of author: Julia Phillips Dickinson

Degree: Master of Science

Program: Communication & Media Technologies

College: Liberal Arts

I understand that I must submit a print copy of my thesis or dissertation to the RIT Archives, per current RIT guidelines for the completion of my degree. I hereby grant to the Rochester Institute of Technology and its agents the non-exclusive license to archive and make accessible my thesis or dissertation in whole or in part in all forms of media in perpetuity. I retain all other ownership rights to the copyright of the thesis or dissertation. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

Print Reproduction Permission Granted:

I, Julia Dickinson, hereby **grant permission** to the Rochester Institute of Technology to reproduce my print thesis or dissertation in whole or in part. Any reproduction will not be for commercial use or profit.

Signature of Author: Julia P. Dickinson Date: 9-11-06

Print Reproduction Permission Denied:

I, _____, hereby **deny permission** to the RIT Library of the Rochester Institute of Technology to reproduce my print thesis or dissertation in whole or in part.

Signature of Author: _____ Date: _____

The following members of the thesis committee approve the thesis of
Julia Phillips Dickinson on August 14, 2006

Susan B. Barnes

Dr. Susan B. Barnes
Department of Communication
Thesis Advisor

Chris Schreck

Dr. Christopher Schreck
Department of Criminal Justice
Thesis Advisor

Bruce Austin

Dr. Bruce Austin
Department of Communication
Chairman

I'm your only friend

I'm not your only friend

But I'm a little glowing friend

But really I'm not actually your friend

But I am

--They Might Be Giants, "Birdhouse in Your Soul"

I turn to my computer like a friend

I need deeper understanding

--Kate Bush, "Deeper Understanding"

Table of Contents

Abstract.....	5
Introduction	6
Literature Review	9
SIDE Theory and Online Codes of Conduct	9
Stalking: Before and After the Internet	14
What Does Cyberstalking Entail?.....	18
Anti-Cyberstalking Movements	24
Cyberstalking on the College Campus	26
Research Questions.....	29
Method.....	30
Results	32
Sample Characteristics	32
What are the Similarities and Differences between Conventional Stalking and Cyberstalking as Seen among RIT Students?.....	35
What are RIT Student Reactions to Cyberstalking Behaviors Versus Conventional Stalking Behaviors?	38
Discussion.....	41
Limitations.....	41
Future Research	42
Conclusion	43
References	47
Appendix 1: Cyberstalking Suvey	52
Footnotes	60
Table 1: Respondent Computer Use	61
Table 2: Respondent Demographics.....	62
Table 3: Respondent Internet Privacy Attitudes.....	63
Table 4: Respondent Reports of Stalking Experiences	64
Table 5: Respondent Reactions to Stalking Experiences	65
Table 6: Respondent Reports of Cyberstalking Experiences	66
Table 7: Respondent Reactions to Cyberstalking Experiences	67
Table 8: Computer Use for Respondents Who Experienced Cyberstalking Incidents.....	68

Abstract

Stalking via the Internet (cyberstalking) occurs via technologies such as email, instant messaging, chat rooms, discussion groups, and social networking websites. Recent news reports indicate a growing concern about the ease with which personal information can be accessed on the Internet – a fact that is shaping new social norms for young adults and children who have grown up using the Internet. This thesis measured the prevalence and nature of cyberstalking among Rochester Institute of Technology students. A survey was conducted and the results were evaluated with SIDE theory and social conduct theory as guides to understand if cyberstalking behavior is becoming normalized among college students or if it is viewed as misbehavior.

The Phenomenon of Cyberstalking on the RIT Campus:

Definitions, Behaviors and Normalization

Stalking via the Internet (cyberstalking) appears to be a growing problem in a world that has a growing dependence on computers and the Internet (Miceli, Santana & Fisher, 2001). Researchers and commentators such as Bocij (2002, 2003) and Hitchcock (2002) have brought cyberstalking cases to the public's attention and have attempted to measure cyberstalking behaviors (Bocij & McFarlane, 2003). Yet some observers doubt whether cyberstalking is significantly serious enough to warrant greater scientific and policy attention. One objection is simple incredulity that cyberstalking victims would read objectionable emails or instant messages that are easy to delete or otherwise ignore (Meloy, 1998). Additionally, critics like Koch (2000) question cyberstalking's validity as a social problem based on a lack of research on the topic.

However, these critical views completely disregard the fact that stalking as a whole is an under-investigated topic (Sinclair & Frieze, 2005). The overall prevalence of stalking in America varies from 2% to 33%, depending on the definitions and measures of stalking being used in a particular study (Williams & Frieze, 2005). But while these differing definitions and approaches make it difficult to easily characterize stalking's prevalence, it is a known and acknowledged social issue. For example, Meloy (1998) found that about half of stalkers threaten their victims with physical harm, and that stalkers do physically assault their victims in about one-third of cases. With these concerns and facts in mind, this thesis aims to better understand the still-emerging, under-researched and greatly debated phenomenon of cyberstalking.

Exploratory research indicated the consequences can be considerable for the victims, just as the effects of conventional stalking are (Bocij & McFarlane, 2003; Morewitz, 2003). For many people in today's society – particularly children and college students who grew up using the Internet – “avoiding” online harassment can constitute giving up personal freedom and capitulating to the stalker, much in the way victims of conventional stalkers find their world growing smaller and smaller through their attempts to evade their pursuer. Also, because women are generally stalked more often than men, women's advocacy groups are concerned about cyberstalking because of the growing number of female Internet users worldwide (Miceli, Santana & Fisher, 2001).

Cyberstalking can cross into the “offline” world as well, as the growing number of cases demonstrates (Bocij, 2002). Recent incidents involving popular social networking websites such as MySpace (<http://www.myspace.com>) have brought cyberstalking in to the public eye within the context of the Internet's greatest horror story: online connections that lead to sexual assault and even murder (AP, 2006). Furthermore, self-reported studies indicate that cyberstalking can have the same negative impact on a victim as conventional stalking (Bocij, 2003; WHOA, 2005).

Stalking involves dysfunctional and destructive human relationships and has a very long history (Bocij, 2003). Mullen, Pathé and Purcell (2000) define stalking as “a constellation of behaviors in which one individual inflicts on another [individual] repeated unwanted intrusions and communications” (p. 7). The definition can be operationalized to include specific measurable behaviors (i.e., the number of unwanted phone calls received from the stalker in a month).

The aim of this thesis is two-fold. First, in order to address the concern that little is known of how prevalent cyberstalking is, it is important to gain exploratory knowledge of cyberstalking's prevalence and nature. Relevant data will come from a sample of students attending the Rochester Institute of Technology (RIT). Second, to verify that cyberstalking has problematic consequences, it is necessary to assess those how disruptive, or perhaps how normalized, cyberstalking is becoming. The present study's literature review discusses two communications theories, SIDE theory and social conduct theory, to see whether or not they relate to possible normalization of cyberstalking behaviors or, conversely, how cyberstalking may be seen as an actionable threat. The rest of the literature review will discuss current cyberstalking research and the definitional conflict over how cyberstalking relates to, but is a separate phenomenon from, conventional stalking. The definition chosen to guide the present research will also be presented. Types of cyberstalking behaviors, cyberstalkers' motivations, as well as criticisms of the cyberstalking phenomenon will also be discussed as well as what victims and law enforcement can do to combat this form of cyber crime. The final section of the literature review will address the Rochester Institute of Technology's current approach to cyberstalking among its students and the factors that informed the survey that were conducted as part of this thesis.

An important theme found in cyberstalking research is how exactly to classify and approach cyberstalking, not only because of the topic's newness, but also because the larger topic of stalking is full of inconsistencies and varying definitions (Williams & Frieze, 2005). And it can be difficult to objectively perceive public views on

cyberstalking because the media regularly sensationalizes the “dark side” of the Internet in the interests of ratings (Miceli, Santana & Fisher, 2001). Stalking researcher Meloy (1998) is clear about stalking’s legitimacy as a social problem, but he also cautioned against alarmist reactions to cyberstalking, noting that “every new technology can serve as a vehicle for criminal behavior” (p. 10). So perhaps the best approach to take is a balanced one. Because cyberstalking is such a new topic, it is important to approach it without bias or alarmist agendas. The present study will strive to take into account both stances before evaluating cyberstalking’s prevalence on the RIT campus.

Literature Review

SIDE Theory and Online Codes of Conduct

Given Meloy’s (1998) caveat about the subjective nature of stalking, it is important to begin the review of cyberstalking literature with a discussion of communications theories that apply to the topic. One of the largest questions within both stalking and cyberstalking theory is how to define the threshold at which a behavior (or group of behaviors) actually *becomes* stalking (Sinclair & Frieze, 2005; Haugaard & Seri, 2004). The larger issue of cyberstalking’s legitimacy as a social problem – despite recent crimes and misbehaviors linked to computer mediated communication (CMC) – has already been mentioned (AP, 2006). The purpose of the present study is to explore cyberstalking among college students – a population generally considered tech-savvy and therefore presumably at greater risk of online victimization than the general population. It

is important to discern not only cyberstalking's prevalence and nature in this high-risk group, but even if students perceive it as a problem.

Social identification/deindividuation (SIDE) theory, which was first set forth by Postmes, Spears and Lea (1998, 2000), can aid in determining whether or not an online behavior (such as cyberstalking) is becoming normalized or if it is considered misbehavior. "Misbehavior" was succinctly defined by Sternberg as "conduct which does not conform to norms and which breaks rules" (Sternberg, 2001, p. 201). SIDE theory is a conglomeration of other theories, including social construction theory, deindividuation theory and social identity theory (Barnes, 2003). Deindividuation theory has been studied extensively within the context of crowd behavior – or more specifically, the actions of individuals *within* crowds (Postmes, Spears & Lea, 1998). Originally it was assumed that individuals in large groups (particularly mobs) lost their ability to evaluate their own behavior and conformed to the group's actions, leading individuals to participate in antinormative behavior (p. 694). However, a meta-analysis that Postmes and Spears (1998) performed on deindividuation research revealed that deindividuation tended to cause the *opposite* effect in large groups, in other words, a greater adherence to established norms. Individuals in crowds and other groups tend to "identify with and see themselves as part of the crowd and the crowd's norms are adhered to more strongly as a result" (Postmes, Spears & Lea, 1998, p. 697).

Building off of this revised understanding of deindividuation, SIDE theory states that in the absence of visual cues, computer users will obey social norms on default. Furthermore, "Group norms and social stereotypes define the limits of social behavior

that are often used to differentiate groups...” (Postmes, Spears and Lea, 1998, p. 690). In other words, when communicating in text-based environments, users tend to rely on the common identity an online group can engender, and that identity is created by the various social norms the group espouses. For example, certain behaviors, such as flaming¹ may be perfectly acceptable in a video games discussion group, but would be looked down upon in a discussion group about pregnancy and motherhood. It all depends on what social norms a specific group operates by. Also, Postmes, Spears and Lea (2000) note that these online group interactions can seem as real as the socialization within a conventional offline group, even though no direct physical contact is taking place. Another assumption users tend to make in the absence of visual contact is that their fellow users are *like* them and will therefore follow the norms of the group as well (Barnes, 2003). As Postmes and colleagues (1998) explained the outcome of an experiment on deindividuation in CMC settings:

Participants showed shifts in the direction of group norms when their shared social identity was made salient and when they were isolated (and anonymous), and shifts away from the group norms when their individual identity was salient when isolated. (p. 699)

In other words, SIDE theory explains how social groups on the Internet have formed their own norms and varying levels of cohesiveness. The fewer opportunities for individuation available to a unique user, the more likely they are to adhere strongly to group norms and assume that the other users are similar to them in intent, beliefs and actions.

What implications does SIDE theory have for cyberstalking? As previously discussed, in the online world, just as in the offline one, people rely on social convention and norms to interact, and there are codes of conduct depending on what situation one is in. But online, people must rely on these norms even more because of the lack of visual interaction. This leads to people making a lot of assumptions about the behavior of other users, as well as seeing themselves as part of a cohesive “in” group (Postmes, Spears and Lea, 1998, p. 690). So users may in fact be more likely to accept certain behaviors as “par for the course” because they have very little choice *but* to accept them in order to continue interacting with others through CMC. Postmes, Spears and & Lea (2000) found that online groups become more cohesive with time and norms develop as well. The present study will consider cyberstalking at RIT within the context of possible normalization. That is, the behaviors are gradually conforming to social norms and are they themselves becoming normal and acceptable. In other words, while tragic cyberstalking cases have occurred, there is the possibility that, due to the SIDE effect, behaviors associated with cyberstalking may largely cease to be considered misbehaviors by those who experience them.

To further understand the group behavior and misbehavior seen in SIDE theory, Gattiker (2001) utilized cognitive development theory to explain individuals’ codes of conduct within online groups. Gattiker noted that the ability to discern right from wrong depends a great deal on how objectively an individual can view situations (p. 104). So despite the assumptions people must make about their fellow users’ similarity to them according to SIDE theory, each individual user may react to a given situation in the

online community differently. Online groups develop their own norms and mores for basic operation (Barnes, 2003). But when looking at specific situations within the group, what may seem like a trivial matter for one member can appear as an egregious breach of conduct to another because each user is judging the situation by their own values in addition to the group's conventions (p. 266).

The necessary adoption of a strict version of norms and conventions allows Internet communities to function cohesively, but this also forces users to make many assumptions about the people they converse with online. When a group of individuals conflicts in a visual cue-free environment, maladaptive and over-compensational behaviors can result because the group members have varying levels of objective perception and their own ideas about norms and codes of conduct (Gattiker, 2001).

Online conduct doesn't end with individual differences among users; misbehavior can also be viewed through the lens of individual conduct, specifically, Gattiker's social conduct theory (2001). Gattiker defined three domains of moral development, all with varying degrees of seriousness and consequence: the Moral Domain (the most serious domain, dealing with actions that do serious harm and that most people can agree are wrong), the Conventional Knowledge Domain (learned by exposure to group norms, and dealing with actions that break those norms, but are usually not harmful), and the Personal Knowledge Domain (acceptable and unacceptable behaviors as learned from an individual's family, generally having no serious consequences in society, but which can lead to misunderstandings) (Barnes, 2003). Gattiker also created a cube model to show varying codes of conduct set forth by various societal forces (Barnes, 2003; Gattiker,

2001). In the present study's conclusion, an assessment will be made of where cyberstalking behaviors fit on Gattiker's moral domain and cube models based on the results of the survey. These classifications will lead to a better understanding of whether to consider cyberstalking a normalized nuisance or looming threat, and how to best manage and prevent cyberstalking. For example, we will see in the present study's results whether students who experienced cyberstalking behaviors reacted by telling the perpetrator to stop, and what further actions they took to end the behaviors (if any).

Stalking: Before and After the Internet

Before we assess cyberstalking among RIT students, we must examine what established research has said about both conventional stalking and cyberstalking. In the preface to his book *The Psychology of Stalking*, Meloy calls stalking "an old behavior, but a new crime" because stalking behaviors have always occurred in society but only recently became prosecutable under law (Meloy, 1998, p. xix). Conventional stalking is a social problem that entered the public consciousness in the 1980's and 1990's, when a rash of celebrity stalking cases led to anti-stalking legislation and increased security measures for famous people and their families (Miller, 2005). During this period, several very public *Othello*-esque situations further added to the misconception that stalking was a problem of the rich and famous. In 1982, up-and-coming actress Dominique Dunne, daughter of society columnist Dominick Dunne, was murdered by an ex-boyfriend who aggressively stalked her in the wake of their breakup (Dunne, 2006). Similarly, the extent to which O.J. Simpson stalked his ex-wife Nicole Brown before her grisly murder is often brought up when his role in her death is discussed (Meloy, 1998; Wurtzel, 1998). While

these highly-publicized cases have certainly raised public awareness of stalking, the vast majority of people who are stalked are not celebrities (Wood & Wood, 2002). A 1999 report on cyberstalking from the U.S. National Institute of Justice (NIJ) indicated that in the United States, "...one out of every 12 women (8.2 million) and one out of every 45 men (2 million) have been stalked at some time in their lives" (National Institute of Justice, 1999, ¶ 21).

As for cyberstalking, the NIJ report merely indicated that there *could be* a huge amount of cyberstalking victims (¶ 20). This seems to be a pattern in the cyberstalking literature: it is a known problem, not much data exists to back up the anecdotal evidence (Bocij, 2003). One reason for this is because cyberstalking is a new phenomenon that did not exist before the Internet became popular (Bocij & McFarlane, 2003). Originally, it was assumed that cyberstalking was a natural extension of conventional stalking; stalkers were merely taking advantage of new communication technologies to harass their victims (Ogilvie, 2000). But as use of the Internet and communications technologies grew, a phenomenon emerged in which individuals were being harassed *exclusively* online, often by total strangers (Bocij, 2003).

Bocij (2002) set forth a basic definition of cyberstalking as "...a new form of behavior where technology is used to harass one or more individuals" (p. 12). As the definition indicates, cyberstalking occurs when victims are harassed, threatened and even monitored using computers and Internet technologies such as email, instant messaging, chat rooms and discussion groups. Cyberstalking can even include property damage, such as the transmission of computer viruses that disable computers (Bocij, 2002). The work

of a few dedicated researchers and victims-turned-advocates has shed light on the confusing subject of cyberstalking, how and why it happens, how it affects victims, and what can be done to locate and prosecute offenders (Hitchcock, 2002). Unfortunately – and not unlike its counterpart conventional stalking – minimal research has been conducted on cyberstalking (Sinclair & Frieze, 2005; Bocij, 2003). Also, differing definitions of cyberstalking exist, which makes it easier for cyberstalking critics to dismiss the problem and also hinders progress towards anti-cyberstalking legislation.

Several researchers have presented definitions of cyberstalking in an attempt to distinguish it from conventional stalking. The definition that acknowledges cyberstalking uniqueness and various forms comes from Paul Bocij, a British IT consultant and leading researcher on the subject. He has encouraged authorities to view cyberstalking as a social problem since the early 2000's. Bocij and his colleague, Leroy McFarlane, (2002) set forth a definition of cyberstalking that encompasses the various types of cyberstalking that will be discussed hereafter.

A group of behaviors in which an individual, group of individuals or organization, uses information and communications technology to harass one or more individuals. Such behaviors may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring, the solicitation of minors for sexual purposes and confrontation. Harassment is defined as a course of action that a reasonable person, in possession of the same information, would think causes another reasonable person to suffer emotional distress (p. 12).

This definition includes all of cyberstalking's main behaviors, which have previously been discussed in this review. The definition also addresses one of cyberstalking's main criticisms: the actual threat cyberstalking presents to society. Detractors such as Koch (2000) insist that cyberstalking poses no real threat to its victims, because the perpetrators are not likely to escalate their activities beyond the online harassment. Aware of these criticisms, Bocij pointed out that pedophiles have employed cyberstalking methods to locate children online for abduction and assault (Bocij & McFarlane, 2003, Bocij, 2002). This observation echoes more recent concerns about predators accessing children's and teenagers' personal information via social networking websites (Sullivan, 2006).

There are several major differences between conventional stalking and cyberstalking. First, we must consider the fact that the Internet makes it very easy to locate and contact people. Building on this fact, a 1999 cyberstalking report from the NIJ stated that cyberstalking can originate wherever the stalker lives and the target can literally be anywhere in the world – as long as the two have access to the Internet. In other words, "...cyberstalkers may be located across the street or across the country" (National Institute of Justice, 1999, ¶ 13), whereas in conventional stalking, the stalker and victim are generally in the same geographic area. Aside from this first major difference, the NIJ report also makes the actual stalking activities easier for the stalker to commit because of the depersonalized nature of computer mediated communication (CMC) (¶ 13). Meloy affirms this view, adding that the cyberstalking options disinhibit

reticent predators because “the Internet allows communication with another person unconstrained by social reality” (Meloy, 1998, p. 11).

What Does Cyberstalking Entail?

To further explore cyberstalking behaviors and victim typologies, Bocij conducted a web-survey (Bocij, 2003). The study asked victims about their own computer proficiency and Internet usage, whether or not they knew their cyberstalkers, and how long the stalking lasted. Bocij found that incidents of cyberstalking take place over shorter periods of time as compared to conventional stalking (within their study, most of the stalkers ended their behaviors within 6 months). Common cyberstalking behaviors included direct harassment via email, instant messenger programs or chat rooms, posting rumors/lies on message boards, and sending viruses to the victim’s computer. Only 33% of the victims reported the stalking to the authorities, and many were concerned their cyberstalking reports wouldn’t be taken seriously (Bocij, 2003). Also, most of the people surveyed (42%) did not know their stalker’s identity. Becoming a stalker’s target can be as confusing as it is terrifying, particularly if the stalker is a complete stranger. Since cyberstalking tends to be perpetrated more often by strangers than people known to the victim, it is important to explore cyberstalking because little research has been done on whether stranger-stalkers or stalkers already known to the victim pose a greater threat for physical violence (Farnham, James & Cantrell, 2000).

As for the cyberstalkers themselves, McFarlane and Bocij (2003) defined four distinct types: Composed, Vindictive, Intimate, and Collective. The Composed cyberstalkers are generally strangers to the victims who want to cause distress – not

establish a relationship. Bocij's research indicates that Composed cyberstalkers are merely looking for a "cheap thrill" and may in fact cyberstalk several victims at the same time (Bocij, 2003). This type of cyberstalker has no true analogous class within conventional stalking. This discovery adds merit to the argument of cyberstalking being separate from conventional stalking.

A Composed cyberstalking case involving a celebrity occurred in 1999, when television actress Jeri Lynn Ryan of *Star Trek: Voyager* fame began receiving hundreds of emails from a supposed fan (McQuade, 2005). The fan was ordered to cease his communications, but he persisted, telling Ryan that he would stop contacting her if she donated a large sum of money to a charity. He even made a video of himself justifying his actions and posted it on his personal website. Two years later, he was convicted under California's stalking law (p. 96). However, the additional charge of extortion and Ryan's celebrity status no doubt helped her case.

The second stalker type, called the Vindictive cyberstalker, is much more aggressive and threatening. The cyberstalking often begins after the stalker has an argument or misunderstanding with the victim. These stalkers are similar to the Resentful stalkers found in conventional stalking, whose aim is to frighten their victim (Mullen, Pathé & Purcell, 2001). Resentful stalkers tend to feel injured or slighted by the person they stalk and are seeking retribution. An example of Vindictive cyberstalking can be found in Jayne Hitchcock's (2002) story of "Nina," a female victim of instant message (IM) cyberstalking. She had difficulty getting campus security to believe her story because the male student responsible claimed they were dating. In fact, they had only

been friends, and that relationship had soured when his obsessive behavior first manifested itself via emailed love poems. Then the cyberstalker's communications took on a malicious tone. "Nina's" case concluded with her moving off-campus to physically get away from the stalker.

A third type of stalker, called the Intimate cyberstalker, tries to win the victim over and/or get retribution after a relationship had ended. Intimate cyberstalkers are three conventional stalker types rolled into one: the Rejected stalkers who are pursuing a former intimate or friend, Intimacy Seekers who are trying to establish a relationship with the victim, and Incompetent Suitors, who are socially myopic and inept and don't usually realize their pursuit is upsetting to their target (Mullen, Pathé & Purcell, 2001). Certainly the detached anonymity of the Internet helps to reinforce the fantasy relationships stalkers often believe they have with their victims (Brownstein, 2000; Meloy, 1998). Parallels to Intimate cyberstalking are seen in the story of Francine Maroukian. A chef and author living in New York City, Maroukian wrote about being stalked for a decade by a neighbor's acquaintance. She only met the man once – then the stalking began. "I know what he looks like...but I don't know where he comes from, how he lives, or why he chose me." (Maroukian, 1998, p. 52).

The fourth type, Collective cyberstalkers, has the most unique motives: they tend to be a group of people working together to discredit someone in an online community or perform corporate espionage. Collective cyberstalkers can also fall under the category of "stalking by proxy," in which one "stalking ringleader" directs an online campaign of harassment and "cyber-smearing" against the victim using other members of a online

community (Bocij & McFarlane, 2002). Again, this type of cyberstalking is not similar to any type of recognized conventional stalking because conventional stalker types are always analyzed on an individual basis (Mullen, Pathé & Purcell, 2000). It seems to be assumed that *one* stalker will pursue *one* victim at a time. Mullen et al (2001, 2000) mention the five main conventional stalker types (Rejected, Intimacy Seeker, Incompetent Suitor, Resentful and Predator) but do not mention the possibility of multiple stalkers pursuing the same target – beyond stalkers who pursue the relatively small population of celebrities.

Another type of cyberstalker that tends to dominate media headlines is analogous to the conventional Predatory stalker – a dangerous individual who intends to harm their target (Mullen, Pathé & Purcell, 2001). One of the first cases of predatory cyberstalking occurred in 1999, when 20-year-old Amy Boyer was gunned down by a former high school classmate, Liam Youens, in the parking lot of the dentist's office where she worked. Youens then shot and killed himself, leaving the entire community of Nashua, New Hampshire in shock (Hitchcock, 2002, Bocij, 2003). Although the two had, to all appearances, barely been acquainted in high school, Liam developed an obsessive "love" for Amy that he harbored long beyond graduation. But he took his obsession to a new level. As Amy's distraught parents discovered after her murder, Liam had a website devoted to his obsession with their daughter, along with increasingly disturbed rants and a tally of the various firearms he owned. Youens found Amy's work address via websites that furnish users with personal information for a fee. Of course, the purported intention of such services is to "reconnect" long-lost relatives and friends, but even Liam noted on

his website that it was staggeringly to find information about people online (Hitchcock, 2002).

Predatory cyberstalking can also be found in several recent cases where several teenagers have been sexually assaulted by individuals they met via the social networking website, MySpace (AP, 2006). There has been ongoing public concern about pedophiles and other sexual predators using the Internet to lure young children since the mid-1990's (Morewitz, 2003). Furthermore, there is growing awareness and concern about just how much personal information young people reveal about themselves online (Sullivan, 2005). A recent study on bloggers⁴ showed that there is a lack of understanding among users about how these technologies actually *work* (Viégas, 2005). Unlike face-to-face conversations, information shared online does not fade with time. So while Viégas (2005) found that users are willing to be accountable for the information they reveal online, they do not seem to understand how persistent that information is (i.e., it remains cached and accessible in servers for years).

The present study focuses on Composed, Vindictive and Intimate cyberstalking behaviors, the prevalence of which can be measured by asking participants if they have experienced certain behaviors and do not require them to admit to any wrongdoing. Also, Intimacy Seekers and Incompetent Suitors often pursue strangers (Mullen, Pathé & Purcell, 2000), so analogous behaviors could be expected from Intimate cyberstalkers. No one who shares their information on the Internet is *asking* to be stalked or assaulted. But individual Internet users are unwittingly making the process much easier because of apparent shifting attitudes on privacy. Sullivan (2006) found that many Internet users,

especially younger users who grew up using the Internet, freely disclose the details of their lives on social networking websites. These same young users lack knowledge of how online information is stored and accessed – in particular, how easy it is for nearly anyone to access information (Sullivan, 2006; Viégas, 2005). While the present study did ask if respondents were ever attacked by someone who stalked them, it was decided that the topic of predatory stalking was too sensitive and complex to explore and would in fact constitute a separate study.

In summation, justification for further research on cyberstalking can be found with cyberstalking theory's critics. In his article *Cyberstalking Hype*, Koch (2000) presents the argument that no credible studies on cyberstalking exist and that the phenomenon is little more than media hype. But Bocij and McFarlane's research (2003, 2002) clearly shows that cyberstalking can cause the same amount of distress as conventional stalking. Furthermore, the information on cyberstalking cases *can* be gathered: anti-stalking groups keep track of their cases, and more and more police departments are devoting energy to cyber crimes. However, this information must be organized analyzed in order to be useful. Also, the stories of the victims themselves, which highlighted much of Bocij and McFarlane's (2002, 2003) research, must be taken into account and not dismissed as hysteria. Bocij (2002) puts it best: "The victims of cyberstalking incidents should not be ignored and the harm suffered by these individuals must not be trivialized" (p. 4). Even if a cyberstalking victim never sees their pursuer face-to-face, it is not uncommon for them to be concerned about theirs and their family's

safety, just as victims of conventional stalking are (Morewitz, 2003). Thus, more research is needed.

Anti-Cyberstalking Movements

Presently online, there are several individuals and organizations actively fighting cyberstalking. In 1996, professional writer Jayne Hitchcock became the target of aggressive cyberstalking after she posted a warning about a shady “literary agency” on a discussion list (Hitchcock, 2002; Goldsborough, 2004). The agency proceeded to post false information about Hitchcock online, “mail bombed”² her email inbox and conventionally stalked her as well. The individuals involved were eventually prosecuted for other illegal activities and Hitchcock’s experience became her impetus to begin an online anti-cyberstalking movement. Her organization, WHOA (Working to Halt Online Abuse, <http://www.haltabuse.org>) provides services to cyberstalking victims free-of-charge (Hitchcock, 2002). Another cyberstalking investigation group is Cyber Angels, which is associated with the vigilante group Guardian Angels (<http://www.cyberangels.org>). Both WHOA and Cyber Angels receive cyberstalking complaints regularly, but the statistics of their own cases are not necessarily considered a good reflection of cyberstalking’s prevalence because neither group has ever conducted formal surveys (Bocij, 2002). WHOA reports their case statistics on their website but also have a disclaimer stating that all their data is from self-reported cases and cannot be verified (WHOA, 2005). These weaknesses in data collection and concrete research reinforce the newness of cyberstalking as an online phenomenon, as well as the importance of strengthening and increasing those data collection efforts.

When it comes to cyberstalking and the law enforcement community, Bocij, Griffiths, and McFarlane (2002) suggest that legislation must be changed to reflect new technologies. Also, they feel that the definition of harassment must be broadened and redefined so as not to disenfranchise cyberstalking victims who have, for example, been harassed but not necessarily threatened (p. 4). Fortunately, advancements are being made to facilitate the capture and prosecution of cyberstalkers. The New York Police department (NYPD) has been facing cyber crime head-on for several years with their Computer Investigation and Technology Unit (CITU) (D'Ovidio & Doyle, 2003). Of all the cases CITU investigated from 2002-2003, cyberstalking made up about 40%. And of those cases, harassment took place mostly through email, with IM coming in a close second (p. 12).

D'Ovidio and Doyle (2003) also advocate the need for better anti-stalking legislation in states where the definition is not wide enough to include cyberstalking behaviors. They suggest computer crime divisions should focus their energies on cyberstalking and encourage police departments to work harder to resolve jurisdiction and extradition issues. They also encouraged Internet service providers (ISP's) to act more responsibly by setting data collection standards for their users' account information so it is easier for investigators to locate suspected stalkers (p. 17). Another concern D'Ovidio and Doyle (2003) voiced was about the growing use of so-called anonymizing Internet tools. These are programs and services that strip online communications of identifying information. Anonymizing tools include anonymous remailers – services that send emails through third-party servers, making them untraceable – and programs that

encrypt a computer's online activity, essentially making a user "invisible" to the rest of the Internet. These tools do have legitimate uses. They can protect whistle-blowers and political dissidents who wish to disseminate information without jeopardizing themselves. But they can easily be used for cyberstalking as well. Like so many other forms of technology, online communication tools are a double-edged sword that throw the importance of *intent* into sharp relief.

Cyberstalking on the College Campus

Gattiker (2001) suggested that online misbehavior is an issue that particularly affects college campuses. Thusly, the present study is concerned with cyberstalking among college students. Conventional stalking is also a concern on the nation's college campuses where there tends to be a high incidence of violence against women (Fisher, Cullen & Turner, 2000). Although stalking is generally a male-on-female crime, recent trends indicate that college stalking incidents are more evenly distributed – but college men underreport being stalked by women because they don't want to be seen as incapable of dealing with the situation themselves (Brownstein, 2000). In fact, it is difficult to find definitive measures of college stalking, as Fisher, Cullen and Turner (2000) noted. The main hurdle encountered in their report was the inconsistent definitions of stalking and stalking behaviors used in previous research.

However, more solid statistics can be found for other forms of on-campus violence. Fisher, Cullen and Turner (2000) concluded that a college with a female population of 10,000 could experience 350 rapes a year or more. But the nature of these crimes presents inherent problems, both to victims and investigators. The complex,

frequently ambiguous social circumstances that lead up to many of these assault, abuse and stalking cases often cause victims to never report the crimes and even rationalize away the true nature of what they experienced (p. iii). Interestingly enough, the prevalence of stalking behaviors in a college setting can be explained by the stalker maturation hypothesis, which states that individuals above the age of 40 are less likely to stalk than younger age groups (Morewitz, 2003). However, stalkers in the 18-25 and 26-40 age cohorts are more likely to engage in violence (p.33). This statistic, coupled with Fisher et al's findings highlight the importance of investigating cyberstalking as an under-researched but potentially serious form of social misconduct that particularly impacts young adults.

So how do these studies and theories apply to RIT students? First and most importantly, RIT is a unique college. It is private, large and technologically focused. Many students develop their attitudes about technology while they attend RIT and not before (McQuade & Fisk, 2005). Statistics from RIT's Information Technology Services (ITS) department indicate that during the past 12 months, the Institute's online traffic averaged between 300 and 400 mbps, or megabits per second (ITS, 2006). RIT's status as a technology and business oriented institute means that much of the student body is Internet and computer savvy. The academic buildings have wireless networks and all dormitories and on-campus apartments are Internet-ready. It is not uncommon for students to construct their own elaborate "set-ups" of computers, servers, and wireless routers to facilitate file-sharing and online gaming. Computer programs such as AIM (AOL Instant Messenger) and MSN Instant Messenger, and websites like Facebook

(<http://www.facebook.com>) and MySpace are so ubiquitous that “adding” new acquaintances to one’s online social network is arguably as common as asking about someone’s major. In fact, college law enforcement departments across the country are now utilizing social networking programs to solve campus crimes, identify suspects, and get wind of potentially disruptive events (like parties that may have underage drinking) before they happen (Duboff, 2006).

RIT’s stalking policy has been in place since 2003. Previously there was only an anti-harassment policy (D. Soufleris, personal communication, December 6, 2005). Cyberstalking is only a part of the stalking behaviors seen on campus. RIT Campus Safety indicated that the cyberstalking cases reported to them usually involve a prior relationship between victim and stalker. There is also the factor of how new technology has effected perceptions of personal boundaries and privacy. Campus Safety noted a growing number of students who put their personal information into a semi-public online forum such as Facebook. They are subsequently shocked when a stranger shows up at their dorm expecting to be “friends” (R. Lezette, personal communication, December 13, 2005). And yet that same “stalker” is confused at the “victim’s” anger. Why would they put their address online unless they were okay with people contacting them? Campus Safety and Student Conduct take these incidents seriously. Sharing detailed personal information is a norm of these social networking and IM communities (Sullivan, 2006). It is not uncommon for students to put biographies and photos of themselves online where just about anyone can access them (p. 2). However, recent news reports tell us that not all

community members will follow those norms because of people's differing moral codes and levels of objectiveness as specified in social conduct theory.

Based on interviews with Campus Safety, Student Conduct and the RIT Women's Center found that the three departments tend to agree that stalking and cyberstalking are underreported crimes because: (a) students often have a hard time understanding what's really happening and (b) the Internet has redefined personal boundaries and privacy. College students who have essentially grown up with the Internet seem to have a hard time understanding that it may not be a good idea to post one's phone number in a public online directory. Many students are easy prey because of their naivety, their desire to be polite and socially accepted, and their level of comfort with technology. Student Conduct reported that students often seem shocked that their public personal information could be used against them (D. Soufleris, personal communication, December 6, 2005).

Research Questions

SIDE theory tells us that computer users' online behavior is guided by group norms, but Gattiker reminds us that individuals or different groups have their own levels of moral and social grounding. Thus, the present study seeks to measure cyberstalking at RIT, not only in terms of its prevalence and nature, but also in terms of its comparison to conventional stalking. Also, contrasting specific questions about students' stalking and cyberstalking experiences will allow cyberstalking to be placed on Gattiker's cube model, further defining cyberstalking as either a nuisance or misbehavior. This way, the extent of cyberstalking's normalization within the RIT student community can begin to be examined. So with this perceptions and the previous stalking and cyberstalking research

discussed in the literature review in mind, this thesis seeks to answer the following questions.

- What are the similarities and differences between conventional stalking and cyberstalking as seen among RIT students?
- Are cyberstalking behaviors perceived as a problem among RIT students?

Method

Using Bocij's 2003 cyberstalking survey and McQuade's 2004 online misbehavior survey as guides, an 8-page multiple choice survey was prepared (See Appendix 1). Bocij's cyberstalking study was chosen as a model because it is an instrument based on accepted research conventions, unlike WHOA's data collection methods, which are based on self-reports from victims with no procedures for control or other observations (WHOA, 2005). McQuade's (2005) computer use and ethics survey served as a model for this survey's format because it was easy for participants to read and follow. Also, Mullen, Pathé and Purcell's (2000) requirement that stalking be unwanted guided specific questions about what respondents may have experienced and how it affected their lives.

The present survey had four sections and took approximately 6-8 minutes to complete. The first section focuses on the respondent's computer and Internet usage. These questions were informed by current computing technology and popular trends in social computing. The second section asks questions about conventional stalking behaviors such as threatening phone calls and being followed. To ensure that the incidents being reported

would be restricted to the time they've been at RIT, the survey asks respondents to only report stalking they have experienced within the last year. The third section asks about cyberstalking experiences the respondent may have had. Again, the time frame is limited to the last year. In both section 2 and 3, if the respondent indicated they experienced any stalking or cyberstalking behaviors, they were asked to complete additional questions about those incidents. The fourth section consisted of three questions measuring the respondent's attitude on Internet privacy. The attitude measurement questions about online privacy were created based on personal conversations with representatives from Campus Safety, the Women's Center and Student Conduct (Lezette, 2005; Soufleris, 2005; Ruben, D., personal communication, December 5 2005). Those three questions reflected the major concerns and conflicts these departments expressed about online privacy and boundary issues. The fifth and final section records respondents' basic demographic information. While WHOA collected more detailed demographic data from cyberstalking victims (like victims' ages and ethnicity), such information was not collected for this study because it would have made it more difficult to maintain respondents' anonymity.

The survey was reviewed and approved by RIT's Institutional Review Board (IRB), which recommended that a consent form be added to the survey because some of the questions were considered highly personal. A copy of this consent form was distributed to all respondents along with an informational flyer from RIT's Women's Center. One hundred seventy surveys were distributed in 8 undergraduate classes. The total sample size was 168 because two incomplete surveys were thrown out.

Results

Sample Characteristics

Out of 168 respondents, 92 were female and 76 were male. Most of the respondents were seniors ($n = 75$), 13 were freshmen, 21 sophomores, 55 juniors, and 2 were graduate students. Eighty-four respondents lived off-campus while 57 lived in on-campus apartments and 27 lived in the dorms. The respondents comprised a convenience sample of undergraduates who were taking liberal arts courses. The male-to-female ratio in RIT's liberal arts courses tends to include a higher proportion of females than is the case in the Institute as a whole. Therefore this approach ought to garner a larger amount of female respondents than males because females tend to experience stalking more than males (Miceli, Santana & Fisher, 2001), which in fact turned out to be the case. Also, although respondents were not asked to report their academic majors in the survey, RIT requires all students to take some liberal arts courses. One might be able to infer that a variety of majors would be accessed by distributing the survey in those classes, although it is impossible to know for certain. Future campus surveys on stalking should record participants' academic majors to find out if certain majors are more prone to cyberstalking incidents than others. Furthermore, Fisher, Cullen and Turner (2000) and Mustaine and Tewksbury (1999) only used females in their stalking samples, while the present study used males as well. Out of the 84 respondents who experienced at least one cyberstalking behavior, 47 were females and 37 were males. The higher incidence among females was expected, because females are stalked more often than males (Mullen, Pathé & Purcell, 2000) and because there were more females in the present sample than males

However, the incidence among males reminds us that stalking behaviors tend to be more equal-opportunity on college campuses (Brownstein, 2000) so males as prospective victims must not be ignored.

The convenience sample has several limitations, one being that it is impossible to generalize data from a convenience sample to the student body of RIT as a whole. Only a probability sample permits generalization. Also, there are known gaps in the sample. For instance, the sample excluded RIT's deaf population who attend the National Technical Institute for the Deaf (NTID). Future cyberstalking research should consider this population, as well as endeavor to include respondents from all of RIT's academic majors. The best way to ensure this would be to randomly select participants from RIT's active student database. Because the present sample was one of convenience, it is only acceptable for the exploratory purposes of this study.

Paired samples t-tests were performed at the 95% confidence level to determine if there were any significant differences between the computer and Internet usage of those who did and did not report cyberstalking. The computer and Internet usage of respondents who experienced cyberstalking behaviors can be found in Table 8. Paired-sample t-tests were also performed to determine if there were any significant differences in computer and Internet use in respondents who reported stalking versus cyberstalking behaviors. No significant differences were found for either t-test. However, the sample's overall computer and Internet habits indicate the importance of technology in the residents' lives. Of the 168 students completing the survey, only four reported using the RIT computer labs. Two of these students using the computer lab did not own personal

computers; these were the only respondents who did not own either a laptop or desktop computer. Two other students who reported owning a laptop and a desktop, respectively, also said they used the labs. It was hoped that correlations between computer ownership versus computer lab use could be run to determine if one group was more likely to experiencing cyberstalking. But since the number of respondents who did not own computers was so small, a correlation would be meaningless.

Twenty-one respondents (12%) rated themselves as having “expert” computer abilities, while 80 (48%) considered themselves “advanced”. Sixty-four (38%) counted themselves as “moderate”, and 4 said they were at a “beginner” level (2%). So the majority of respondents considered themselves to be computer-literate and even above-average. Respondents’ rate of taking their computer with them in their daily lives varied greatly. Seven (4%) “always” took it with them, while 16 (10%) “almost always” did. 52 respondents took it “sometimes” (31%) while 27 (16%) “almost never” took their computer with them and 65 (39%) “never” took their computers to class, work, or other out-of-home locations.

One-hundred forty-six respondents (80%) either agreed or strongly agreed that a computer was important to their everyday lives. Similarly, 151 respondents (90%) agreed or strongly agreed that the Internet was important to their day-to-day lives. Given email’s ubiquity, it was not surprising that over 80% of the respondents checked their email 2-3 times a day or more. No one said that they did not use email. However, the usage of other social computing software – the anecdotal source of much cyberstalking and “online drama” – was varied. About 50% (59) respondents reported logging in to AOL Instant

Messenger or another IM program for the entire day, while only 8% did not use IM at all. Twenty-five percent of respondents said they did not use Facebook at all, and 35% said they logged in 1-2 times a week or less. Thirty-three percent used Facebook 2-3 times a day or more, while only 6% logged in for the whole day. For MySpace, 56% of respondents did not even have accounts, and those who did logged in more infrequently (28% 1-2 times a week or less; only 15% logged in more than one a week). Likewise with blogs (personally hosted, or hosted by a blog service such as LiveJournal or Xanga), 79% of respondents did not have a blog, and 6% used their blogs once a day or more. MySpace is currently more popular among highschoolers (AP, 2006), while Facebook was originally launched for college students only. Thus, students who are currently starting college may be more likely to use MySpace than Facebook. The rest of the results will be discussed by answering the research questions.

What are the Similarities and Differences between Conventional Stalking and Cyberstalking as Seen among RIT Students?

Fifty-seven percent of the respondents who were victims of cyberstalking also experienced conventional stalking. A significant minority (33% of the total sample) did not experience either conventional stalking or cyberstalking. In the overall sample, only 26% experienced any conventional stalking within the last year. Similar to Bocij's research (2003), the present study found that 33% of respondents who experienced cyberstalking said the offenders were strangers. However, in the present study, respondents who experienced conventional stalking similarly did not know their pursuers 34% of the time. A paired-samples t-test was run to explore possible differences between

how respondents who experienced stalking versus cyberstalking reacted to the incidents. Respondents who experienced stalking did report the stalking to Campus Safety in 9% of cases versus 1% of cyberstalking cases, $F(1, 80) = .038, p < .05$. Also, 3 stalking respondents utilized written letters to tell the stalker to stop, versus no cyberstalking respondents. Also in keeping with the online nature of cyberstalking, 16 cyberstalking respondents versus 4 stalking respondents told the stalker to stop via IM. Conversely, 22 stalking versus 4 cyberstalking respondents told the stalkers to stop in person. This infers that stalking that starts online tends to be resolved online, and conventional stalking tends to be resolved through more traditional and/or face-to-face communication. A detailed outline of respondent reactions to stalking experiences can be found in Table 5.

Table 6 reports the prevalence of the different subcategories of cyberstalking behaviors. While half of the sample experienced at least one cyberstalking incident, only a much smaller fraction experienced multiple instances of victimization during the previous year. Of those who were victims during the previous year, 10 (12%) had received threatening email and 8 (10%) received threatening emails twice or more. Fourteen (17%) got threatening emails once, and 10 (12%) received such emails two or more times. Fourteen respondents (17%) experienced IM threats once, 9 (11%) twice and another 9 (11%) three times or more. 23% of respondents (19) said they'd received abusive IM messages once, 9 (11%) got them twice and 14 (17%) experienced them 3 or more times. Seven (8%) reported having threats made against them once in chat rooms, while 3 (2%) received such threats two or more times. The exact same respondents reported having threats made against them in chat rooms once (7) and twice or more (3).

Six respondents (7%) had threats made against them once via a social networking website, and 3 (3%) experienced such threats two or more. Four (5%) received abusive comments once under the same circumstances, and 3 (3%) experienced them twice or more. Thirteen respondents (15%) said their reputation had been damaged once by information spread online, and 4 more (5%) had such an incident occur twice or more. 10 (12%) have been impersonated online once, and 6 (7%) respondents were impersonated two or more times. Three respondents (4%) reported being “ganged up on” online by people who’d been encouraged to harass them by someone else, and 6 (7%) said they’d been “ganged up on” twice or more. Five (6%) had goods or services ordered in their name without their knowledge one time, and 2 (2%) had this happen three times or more. Fourteen respondents (17%) said someone intentionally sent them a computer virus once, 11 (13%) were sent viruses twice or more, and 6 (7%) weren’t sure if they’d intentionally been sent a virus. Five respondents (6%) were followed by someone claiming they found the respondent’s schedule online, and one respondent was once followed back to their home by someone who found their address online. Eleven respondents (13%) felt in fear for their safety due to the cyberstalking incidents they’d experienced, and 8 (9%) said they’d changed parts of their daily routine because of those incidents. Finally, 10 respondents (12%) adopted personal security measures on one occasion due to their experiences, and 5 more (6%) took personal security measures twice or more.

The results clearly indicate that the cyberstalker is not often unknown to the victim. Only 22 respondents (33%) said a stranger was responsible for the incidents they experienced, while 15 (22%) attributed them to a former friend, 7 (10%) to a current

friend, 14 (21%) to a classmate, coworker or acquaintance, 6 (9%) to a former significant other and 3 (5%) to a current significant other. Twenty-seven respondents (37%) said all the incidents could be traced to the same person, 15 (20%) were perpetrated by mostly the same people, 10 (13%) were done by some of the same people, 3 (4%) were by a few of the same people and 19 (26%) were all done by different people.

What are RIT Student Reactions to Cyberstalking Behaviors Versus Conventional Stalking Behaviors?

Half of the respondents (n = 84) reported experiencing *at least one* cyberstalking incident within the last year. These findings are well above the rates found in other college stalking studies. Fisher, Cullen and Turner (2000) reported a conventional stalking incidence rate of just over 13% among their sample of 581 female undergraduates. Fisher et al's (2000) study included unwanted emails among its stalking criteria. The only cyberstalking metric Fisher and associates measured was the prevalence of stalking via email, which was found to be about 25%. This difference between the current study's prevalence estimates and the extant literature could be due to the cyberstalking focus of the present study (18 questions about cyberstalking behaviors versus one). Other researchers (e.g., Sinclair and Frieze, 2005; Haugaard and Seri, 2004) investigating intrusive and obsessive behavior in young adult relationships noted that definitions of stalking vary widely. Looser definitions and broader ranges of stalking behaviors would make respondents more likely to identify an experience they had as "stalking" (Williams & Frieze, 2005). Therefore, the broader range of stalking behaviors defined in the present study yielded a higher rate of prevalence.

Additionally, it is important to keep in mind that college students tend to display higher rates of stalking behaviors than the general population (Haugaard & Seri, 2004). Morewitz's stalker maturation hypothesis highlighted this stalking prevalence among younger age cohorts, but also noted that as individuals age, they are less likely to engage in stalking (2003). This is possibly due to college socialization factors already discussed in the literature review.

The results also show that cyberstalking is not a phenomenon that students continually experience. Only 12% (9) said they were currently experiencing cyberstalking incidents while 88% (65) were not. Thirty-nine percent of respondents (53%) said the incidents lasted a week or less, 20 (27%) said they lasted 1-4 weeks, 7 (10%) reported them lasting 1-3 months, 4 (5%) said it lasted 3-6 months and another 4 (5%) respondents said they'd experienced cyberstalking behaviors for 6 months or longer. Victims often responded directly to the stalker. Fifty-seven percent (42) of respondents told the person responsible to stop, while 43% (32) never told them. Of the respondents who confronted their stalker, 3 (11%) did so via email, 16 (59%) via IM, one left the stalker a message on a social networking site, 2 (7%) called them, 4 (15%) told them in person, and 1 (4%) asked someone they knew to tell the person to stop. In most cases, the confrontation was sufficient to end the incident. Sixty percent of respondents said the victimization ceased after they told the person to stop, while 17 respondents (40%) said the behaviors did not cease. Respondents overwhelmingly did not turn to formal institutions to respond to cyberstalking on their behalf. Only one respondent reported any cyberstalking to Campus Safety, and none reported any cyberstalking to the

Women's Center. And although 50% of all respondents could report experiencing some form of cyberstalking incident, most did not suffer particularly dramatic negative consequences from their experiences. In fact, 35 respondents (47%) who experienced at least one cyberstalking incident said the experience did not negatively affect their lives. Twenty-eight respondents (38%) said the cyberstalking experiences had a moderately negative impact on them, while 11 respondents (15%) reported it had a negative or very negative affect.

To further measure the possibility of cyberstalking's normalization, the survey asked three questions on the survey to measure respondent attitudes about using information that is found online. Out of the total sample, 35 (21%) strongly agreed that the Internet makes it too easy to find people's personal information. Eighty-four (50%) agreed with the statement, while 43 (26%) were neutral, and 5 (3%) disagreed. Only 7 respondents (4%) strongly agreed with the statement, "If people chose to make their personal information public on the Internet, then it is not wrong when someone they don't know uses that information." Fifty-one respondents (30%) agreed with the statement, 38 (23%) felt neutral, 49 (29%) disagreed and 23 (14%) strongly disagreed. For the last statement, "I would contact someone I had not previously met in person if I found their contact information online" 5 respondents (3%) strongly agreed, 30 (18%) agreed, 37 (22%) were neutral, 55 (33%) disagreed and 41 (24%) strongly disagreed. While these measures yielded interesting answers, they did not take into account the need to sometimes contact strangers for matters such as employment or service inquiries. Unsolicited use of personal information is sometime not only acceptable, but necessary.

The results of the present study show that people who experience cyberstalking are often strangers to their pursuers, as noted in Bocij and McFarlane's cyberstalking definition (2002). However, conventionally stalked respondents were stalked by strangers at nearly the same rate. It appears that, generally speaking, some cases of cyberstalking at RIT resemble the Bocij and McFarlane definition, while other cases may be closer to researchers like Ogilvie (2000) who say cyberstalking merely augments conventional stalking. And unlike Bocij's (2003) findings, the majority of cyberstalking behaviors took place via IM, while there was minimal reporting of other incidents, which could lead us to conclude that cyberstalking incidents at RIT usually consist of one or two behaviors that usually last less than a month.

Discussion

Limitations

The present study only had 168 participants. While this was enough to perform valid statistical analyses, future research must include a larger sample. Also, the present study did not differentiate between hearing and deaf/hard-of-hearing participants. RIT has a large deaf/hard-of-hearing population because the National Technical Institute for the Deaf (NTID) is located at RIT. Future studies should include, or focus specifically on, this population to see if their rates of stalking and cyberstalking differ from hearing students'.

Future Research

The one extreme cyberstalking case seen in the present study provides direction to how Women's Center and Campus Safety can approach and further research cyberstalking. Because the results of this study have shown that cyberstalking behaviors are becoming normalized on the RIT campus, the Women's Center and Campus Safety should focus on the extreme cases. One way of doing this would be to conduct a joint stalking study by comparing detailed interviews of students who report and are responsible for stalking of all kinds. This approach would allow researchers to glean very specific information about the cases. A cyberstalker's motives are best understood through interviewing their victims, or interviewing the stalker themselves. However, Sinclair and Frieze (2005) caution that many stalkers, particularly those seeking a relationship with their targets, do not view their actions as inappropriate. Here again, SIDE theory and codes of conduct can be used to understand a cyberstalker's motives. And of course, more research at RIT should include a larger sample size and both males and females, since males did show an incidence rate not much lower than the females' rate.

Most respondents agreed that it was easy to find people's personal information online, while attitudes about contacting people were murkier, with varying degrees of disagreement with the statements. However, Viégas (2005) has found that beliefs and actions in online activities are often contrary. Student beliefs and actual behaviors regarding Internet and computer usage would be an interesting area to explore further.

Conclusion

Bocij, McFarlane, Hitchcock and others have legitimized cyberstalking as an online phenomenon. However, it is important to define the difference between a *phenomenon* and a *problem*. Most of the cyberstalking incidents reported in the present study were experienced only once (see Table 6) and/or were perceived by respondents as only mildly distressing. So while cyberstalking behaviors do occur among RIT students, they are generally not considered problematic by those to experience them and do not persist for long periods of time or culminate in tragic confrontations. Furthermore, Sinclair and Frieze (2002) suggest there is a spectrum of stalking activities that range from normal courtship behaviors to obsessional and obtrusive actions. However, Sinclair and Frieze also note that stalking is often a matter of perception, and the idea of simply pursuing a relationship with someone – be it friendly or romantic – is not always seen in a negative light (p. 840). Building on this concept of perception, the results of the present study show that cyberstalking at RIT mostly occurs episodically and that respondents who experienced cyberstalking behaviors are not upset by them enough to seek help from Campus Safety or the Women’s Center. Fisher et al’s (2000) observed that victims of interpersonal violence like stalking often have difficulty characterizing their experiences as crimes. But it seems that the respondents in the present study had no difficulty characterizing their cyberstalking experiences and made the decision to tell the perpetrator to stop or not. While there was a nearly 50-50 split between respondents telling the cyberstalker to stop or not, the fact that only one respondent reported their

experiences to Campus Safety and that no respondents contacted the Women's Center is indicative of the normalizing of cyberstalking behaviors among RIT students.

Judging by the types of cyberstalking incidents students reported, it seems that cyberstalkers at RIT best fit in to the Composed, Vindictive or Intimate categories since most reported being cyberstalked by strangers (Composed or Intimate motives), acquaintances (Intimate motives) and former intimates (Vindictive or Intimate motives). No evidence of Predatory cyberstalking was found because no students reported being physically assaulted by the perpetrator and only 2% reported being followed home by their cyberstalkers. It should be noted there was one case of a respondent being persistently stalked and cyberstalked by a current significant other. This case accounts for the 1% incidence of a respondent being followed home by their cyberstalker three or more times. The respondent in question was also the only one who reported their cyberstalking experiences to Campus Safety.

Taking all these findings into consideration, Gattiker's domains of moral development can now be revisited. The domain that best fits cyberstalking is the Conventional Knowledge Domain in which morals are learned by observing the group's consensus on various issues. Uniformity and conformity issues are addressed in this domain, but the conditions of behavior can change and breaking these conditions does not lead to serious harm or serious consequences (Gattiker, 2001). So while infractions in this moral domain will be viewed negatively, the only consequence an individual may face is requests by fellow group members to cease the behavior – or, at the very worst, exclusion from the group. Cyberstalking at RIT can now be placed on Gattiker's (2001) cube model

for codes of conduct. There are three levels in the model: justice and public good, specificity of code of conduct and level of regulation (Barnes, 2003; Gattiker, 2001). The model places cyberstalking on the low level for specificity of code of conduct because it breeches social norms and not mores (norms will be perceived with varying degrees of importance by different people, as stated in social conduct theory). Cyberstalking is also at a low level for regulation because of the nebulous accessibility and regulation of information online. Finally, cyberstalking as seen in the present study is low on justice and public good. Gattiker (2001) deems behaviors such as threatening emails are in fact worthy of official and decisive action. But the ways respondents in the present study reacted to their cyberstalking experiences indicate that not only did they not think their experiences were disturbing enough to contact authorities, they generally solved the conflict on their own. Thus, cyberstalking fits in the D quadrant of Gattiker's cube model. Ultimately, SIDE theory and social conduct theory can aid in the understanding of the behaviors that define cyberstalking. Because users rely on the norms of an online group to function in the absence of visual cues (SIDE theory), the detached nature of CMC disinhibits individuals already functioning with lower levels of moral grounding and makes them more likely to misbehave (social conduct theory).

While the media often touts online communication as the tool of depraved predators (AP, 2006), digital technologies in fact have many positive prospects for education. The negatives of online communication have been discussed here in detail, but we must not give in to the alarmist attitude the media often presents. Yes, there have been some tragic and, more common, bizarre cases attributed to cyberstalking, and there is

good reason to pursue it as a criminal offense. But it is important to recall Meloy's (1998) observation about taking the good with the bad when it comes to technology. And it is equally as important to draw the line between true cyberstalking and awkward social situations facilitated by the anonymity and ease of online communication. Perhaps the best way to prevent stalking and cyberstalking at RIT would be to include a cyber ethics unit in First Year Enrichment courses, which would be an excellent opportunity for both departments to get "face time" with students and hopefully encourage more stalking victims to report their experiences. Online communication, whatever form it comes in, is here to stay. It is the responsibility of educators, parents and law enforcement officials alike to understand these technologies and help young people understand the consequences of what they do online.

References

- Associated Press. (February 21, 2006). Teens at risk on social Web sites. Retrieved 21, 2006, from: <http://www.cnn.com/2006/TECH/Internet/02/21/myspace.dangers.ap/index.html>
- Barnes, S. (2003). Computer mediated communication: Human-to-human communication across the Internet. Boston: Pearson Education.
- Bocij, P. (2003). Victims of cyberstalking: An exploratory study of harassment perpetuated via the Internet. *First Monday*, 8(10). Retrieved December 19, 2004, from http://firstmonday.org/issues/issue8_10/bocij/index.html.
- Bocij, P., and McFarlane L. (2003). Seven fallacies about cyberstalking. *Prison Service Journal*, (149), 37-42.
- Bocij, P. (2002). Corporate cyberstalking: An invitation to build theory. *First Monday*, 7(11). Retrieved January 10, 2005 from http://firstmonday.org/issues/issue7_11/bocij/index.html.
- Bocij, P., Griffith, M. & McFarlane, L. (2002). Cyberstalking: A new challenge for criminal law. *The Criminal Lawyer*, (122), 3-5.
- Bocij, P. & McFarlane, L., 2002. Online harassment: Towards a definition of cyberstalking. *Prison Service Journal*. (139), 31-8.
- Brownstein, A. (2000). In the campus shadows, women are stalkers as well as the stalked. *Chronicle of Higher Education*, 47(15), A40-A43.
- D'Ovidio, R., & Doyle, J. (2003). A study on cyberstalking: Understanding investigative hurdles. *FBI Law Enforcement Bulletin*, 72(3), 10-17.

- Duboff, J. (2006). Throwing the “book” at them. *Current Magazine*. Retrieved April 20, 2006 from <http://www.msnbc.msn.com/id/12209620/sire/newsweek/>
- Dunne, D. (May 2006). You’re nobody till somebody bugs you. *Vanity Fair*, 549, 94-98.
- Farnham, F.R., James, D.V., Cantrell, P. (2000). Association between violence, psychosis, and relationship to victim in stalkers. *Lancet*, 355(9199), 1999.
- Fisher, B. S., Cullen, F. T., & Turner, M. G. (2000). *The sexual victimization of college women* (NCJ-182369). Washington, DC: U.S. Department of Justice, National Institute of Justice and Bureau of Justice Statistics.
- Gattiker, U.E. (2001). *The Internet as a diverse community: Cultural, organizational, and political issues*. Mahwah, NJ: Lawrence Erlbaum Associates.
- Goldsborough, R. (2004). Fighting back against cyberstalking. *Black Issues in High Education*, 21(11), 37.
- Hitchcock, J.A. (2002). *Net crimes and misdemeanors*. Medford, NJ: Information Today, Inc.
- Koch, L. (2000, May 29). Cyberstalking hype. *Interactive Week*, 7(21), 28.
- Langhinrichsen-Rohling, J., Palarea, R.E., Cohen, J., Rohling, M.L. (2000). Breaking up is hard to do: Unwanted pursuit behaviors following the dissolution of a romantic relationship. *Violence and Victims*, 15, 73-90.
- Maroukian, F. (August 1998). Call us when he kills you. *Esquire*, 130(2), 52-57.
- McFarlane, L., & Bocij, P. (2003). An exploration of predatory behavior in cyberspace:

towards a typology of cyberstalkers. *First Monday*, 8(9). Retrieved December 19, 2004, from http://firstmonday.org/issues/issue8_9/mcfarlane/index.html.

McQuade, S.C. (2006). *Understanding and managing cybercrime*. New York: Allyn & Bacon.

McQuade, S.C., & Fisk, N. (December 8, 2005). *The RIT computer use and ethics survey*. Research presentation at the Rochester Institute of Technology, Rochester, NY.

Meloy, J.R. (1998). The psychology of stalking. In J.R. Meloy (Ed.), *The psychology of stalking: Clinical and forensic perspectives* (pp. 1-23). New York: Academic Press, Harcourt Brace & Company.

Miceli, S.L., Santana, S., Fisher, B. (2001). Cyberaggression: Safety and security issues for women worldwide. *Security Journal*, 14(2), 11-27.

Miller, M. (2005, February). Stalker Patrol. *W*, 34(2), 130-134.

Morewitz, S. (2003). *Stalking and violence: New patterns of trauma and obsession*. New York: Kluwer Academic/Plenum Publishers.

Mullen, P., Pathé, M., Purcell, R. (2001). Stalking: New constructions of human behaviour. *Australian and New Zealand Journal of Psychiatry*, 35, 9-16.

Mullen, P., Pathé, M., Purcell, R. (2000). *Stalkers and their victims*. Cambridge, UK: Cambridge University Press.

Mustaine, E. & Tewksbury, R. (1999). A routine activity theory explanation of women's stalking victimizations. *Violence Against Women*, 5(1), 43-62.

National Institute of Justice. (1999). *Cyberstalking: A new challenge for law*

- enforcement and industry, a report from the Attorney General to the Vice President, (August 1999). Retrieved February 4, 2005 from <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>
- Ogilvie, E. (2000). Cyberstalking, *Trends and Issues in Crime and Criminal Justice*, (116).
- Online Harassment/Cyberstalking Statistics (2005). Retrieved April 11, 2006 from <http://whoa.femail.com/resources/stats/index.shtml>.
- Postmes, T., Spears, R., Lea, M. (2000). The formation of group norms in computer-mediated communication. *Human Communication Research*, 26(3), 341-372.
- Postmes, T., Spears, R., & Lea, M. (1998). Breaching or building social boundaries? SIDE-effects of computer mediated communication. *Communication Research*, 25(6), 689-715.
- Postmes, T. & Spears, R. (1998). Deindividuation and anti-normative behavior: A meta-analysis. *Psychological Bulletin*, 123, 238-259.
- Sinclair, H.C., Frieze, I.H. (2005). When courtship persistence becomes intrusive pursuit: Comparing rejecter and pursuer perspectives of unrequited attraction. *Sex Roles*, 52(11/12), 839-852.
- Sinclair, H.C., Frieze, I.H. (2002). Initial courtship behavior and stalking: How should we draw the line? In K.E. Davis, I. Frieze, R.D. Maiuro (Eds.), *Stalking: Perspectives on victims and perpetrators* (pp. 186-211). New York: Springer Publishing Company.
- Spitzberg, B., Cadiz, M. (2002). The media construction of stalking stereotypes.

Journal of Criminal Justice and Popular Culture, 9(3), 128-149.

- Sternberg, J.L. (2001). Misbehavior in cyber places: The regulation of the online conduct in virtual communities on the Internet. (Doctoral dissertation, New York University, 2001). *UMI Dissertation Services*, 3022160.
- Sullivan, B. (2006, March 29). Kids, blogs and too much information. Retrieved March 30, 2006 from <http://www.msnbc.msn.com/id/7668788>.
- Viégas, F.B. (2005). Bloggers' expectations of privacy and accountability: An initial survey. *Journal of Computer-Mediated Communication*, 10(3), article 12. Retrieved April 20, 2006 from <http://jcmc.indiana.edu/vol10/issue3/viegas.html>.
- Williams, S.L., Frieze, I.H. (2005). Courtship behaviors, relationship violence, and breakup persistence in college men and women. *Psychology of Women Quarterly*, 29, 248-257.
- Wood, R.A. & Wood, N.L. (December 2002). Stalking the stalker: A profile of offenders. *FBI Law Enforcement Bulletin*, 71(12), 1-7.
- Wurtzel, E. (1998). *Bitch: In praise of difficult women*. New York: Anchor Books.

Appendix 1

Cyberstalking Survey

Survey on RIT Students and Internet Use

This survey is being conducted by an RIT Communications graduate student for her thesis project.

Circle only one answer per question, unless otherwise indicated. If you can't remember a specific number or event, please estimate. **This survey is anonymous.**

First, here are some questions about how you use computers and the Internet:

1. What type of computer do you own?
 - a. Desktop
 - b. Laptop/notebook
 - c. I don't own a computer

↓

Answer question 2 only if you answered C to question 1

2. If you do not own a computer, do you:
 - a. Use the RIT computer labs
 - b. Use a computer belonging to a friend, roommate or significant other

For questions 3 and 4, please indicate your attitude about each statement on a scale of 1-5 with 1 = "strongly disagree" and 5 = "strongly agree".

3. Having access to a **computer** is important to my day-to-day life.
1_____ 2_____ 3_____ 4_____ 5_____
4. Having access to the **Internet** is important to my day-to-day life.
1_____ 2_____ 3_____ 4_____ 5_____
5. Please rate your computer abilities
 - a. Expert
 - b. Advanced
 - c. Moderate
 - d. Beginner
6. In your day-to-day life, how often do you take your computer with you?
 - a. Always
 - b. Almost always
 - c. Sometimes
 - d. Almost never
 - e. Never

Now we'd like to ask you about the websites and computer programs you use:

7. How often do you check your email?
 - a. I do not use email
 - b. More than three times a day
 - c. Two or three times a day
 - d. Once a day
 - e. Once or twice a week
 - f. Less than once a week

8. How often do you log on to AIM or another instant messenger (IM) program?
 - a. I do not use an IM program
 - b. I log on for the entire day
 - c. More than three times a day
 - d. Two or three times a day
 - e. Once a day
 - f. Once or twice a week
 - g. Less than once a week

9. How often do you log on to Facebook?
 - a. I do not use Facebook
 - b. I log on for the entire day
 - c. More than three times a day
 - d. Two or three times a day
 - e. Once a day
 - f. Once or twice a week
 - g. Less than once a week

10. How often do you log on to MySpace?
 - a. I do not use MySpace
 - b. I log on for the entire day
 - c. More than three times a day
 - d. Two or three times a day
 - e. Once a day
 - f. Once or twice a week
 - g. Less than once a week

11. How often do you log on to your blog? (this includes LiveJournal, Xanga, Blogger, or a self-hosted blog)
 - a. I do not have a blog
 - b. I log on for the entire day
 - c. More than three times a day
 - d. Two or three times a day
 - e. Once a day
 - f. Once or twice a week
 - g. Less than once a week

Now we'd like to ask you some questions about experiences you may have had. Again, this survey is anonymous.

For each item, indicate with an X how many times *during the past year* you personally experienced any of the incidents listed.

Type of Incident	Never (0)	Once (1)	Twice (2)	Three times or more (3+)	Not sure
12. I have received threatening letters through the postal mail					
13. I have received abusive letters through the postal mail					
14. I have had my reputation damaged rumors by that were spread by one or more individuals					
15. I have received threatening phone calls					
16. I have received abusive phone calls					
17. I have been followed during my daily routine					
18. I have been followed back to my home, apartment, or dorm room					
19. I have been confronted face-to-face by a person who followed me					
20. I have been physically attacked by a person who followed me					
21. I have felt in fear for my safety and well-being because of the incidents I've experienced					
22. I have changed parts of my daily routine because of the incidents I've experienced					
23. I have adopted personal security measures because of the incidents I've experienced					



If you answered "Never (0)" to all Questions 12-23, please go to Question on Pg. 5

24. The person responsible for these incidents was a (please circle all that apply):

- a. Stranger
- b. Former friend
- c. Friend
- d. Classmate, coworker or acquaintance
- e. Former significant other
- f. Current significant other

25. Thinking back to the list of incidents above, how many of the incidents you experienced could be linked to the same person or same group of people?
- All
 - Most
 - Some
 - A few
 - None
26. Are you currently experiencing any of the incidents listed above?
- Yes
 - No
27. What is the longest amount of time that you experienced these incidents?
- A week or less
 - 1-4 weeks
 - 1 month-3 months
 - 3-6 months
 - 6 months to a year
28. Have you ever told the person/people responsible for these incidents to stop?
- Yes
 - No
29. If you answered "yes" to Question 28, how did you contact them? (please circle all that apply)
- Sent a letter
 - Email
 - IM
 - Left them a message on a social networking site
 - Phone call
 - In person
 - Asked a friend, roommate, or your significant other to confront them for you
30. If you answered "yes" to Question 28, did the incidents end after you confronted them?
- Yes
 - No
31. Did you report the person/persons to Campus Safety?
- Yes
 - No
32. Did you report the person/persons to the Women's Center?
- Yes
 - No

For statement 33, please indicate your attitude on a scale of 1-5 with 1 = “strongly disagree” and 5 = “strongly agree”.

33. My life was negatively affected by the incidents I experienced.

1_____ 2_____ 3_____ 4_____ 5_____

Next, we’d like to ask you some questions about Internet and computer-related experiences you may have.

For each question, indicate with an X how many times during the past year you personally experienced any of the incidents listed.

Type of Incident	Never (0)	Once (1)	Twice (2)	Three times or more (3+)	Not sure
34. I have received threatening e-mail					
35. I have received abusive email					
36. I have had threats made against me via AIM or another IM program					
37. I have had abusive comments made against me via AIM or another IM program					
38. I have had threats made against me in a chat room					
39. I have had abusive comments made against me in a chat room					
40. I have had threats made against me on a social networking website					
41. I have had abusive comments made against me on a social networking website					
42. I have had my reputation damaged by rumors that were posted online					
43. I have been impersonated online					
44. I have been “ganged up on” online by people who were encouraged to harass me					
45. Someone order goods or services online in my name without my knowledge or permission					
46. Someone intentionally sent me a computer virus (not junk mail/spam)					
47. I have been followed during my daily routine by someone who said they found my schedule online					

48. I have been followed back to my home, apartment, or dorm room by someone who said they found my address online					
49. I have felt in fear for my safety and well-being because of the incidents I've experienced					
50. I have adopted personal security measures because of the incidents I've experienced					

↓
If you answered “Never (0)” to all Questions 34-51, please go to Question 62 on Pg. 7

51. The person responsible for these incidents was a (please circle all that apply):

- a. Stranger
- b. Former friend
- c. Friend
- d. Classmate, coworker or acquaintance
- e. Former significant other
- f. Current significant other

52. Thinking back to the list of incidents above, how many of the incidents you experienced could be linked to the same person or same group of people?

- a. All
- b. Most
- c. Some
- d. few
- e. None

53. Are you currently experiencing any of the incidents listed above?

- a. Yes
- b. No

54. What is the longest amount of time that you experienced these incidents?

- a. A week or less
- b. 1-4 weeks
- c. 1 month-3 months
- d. 3-6 months
- e. 6 months to a year

55. Have you ever told the person/people responsible for these incidents to stop?

- a. Yes
- b. No

↓

56. If you answered “yes” to Question, how did you contact them? (please

circle all that apply)

- a. Sent a letter
- b. Email
- c. IM
- d. Left them a message on a social networking site
- e. Phone call
- f. In person
- g. Asked a friend, roommate, or your significant other to confront them for you

57. If you answered "yes" to Question, did the incidents end after you confronted them?

- a. Yes
- b. No

58. Did you report the person/persons to Campus Safety?

- a. Yes
- b. No

59. Did you report the person/persons to the Women's Center?

- a. Yes
- b. No

For statement 33, please indicate your attitude on a scale of 1-5 with 1 = "strongly disagree" and 5 = "strongly agree".

60. My life was negatively affected by the incidents I indicated

1_____ 2_____ 3_____ 4_____ 5_____

Below are a series of statements about privacy on the Internet. Please indicate how much or little you agree with each statement.

61. The Internet makes it too easy to find personal information about people

- a. Strongly agree
- b. Agree
- c. Neutral
- d. Disagree
- e. Strongly disagree

62. If people chose to make their personal information public on the Internet, then it is not wrong when someone they don't know uses that information

- a. Strongly agree
- b. Agree
- c. Neutral
- d. Disagree
- e. Strongly disagree

63. I would contact someone I had not previously met in person if I found their contact information online

- a. Strongly agree
- b. Agree
- c. Neutral
- d. Disagree
- e. Strongly disagree

Finally, please tell us a bit about yourself:

64. I am:

- a. Female
- b. Male

65. I am a:

- a. Freshman (first year)
- b. Sophomore (second year)
- c. Junior (third year)
- d. Senior (fourth/fifth year)
- e. Graduate student

66. I live:

- a. In the dorms
- b. In an on-campus apartment (includes Racquet Club and the RIT Inn)
- c. Off-campus

If you have or currently are experiencing stalking or cyberstalking, please do not hesitate to contact Campus Safety or the Women's Center.

That's all! Thank you!

Footnotes

¹Flaming occurs when individuals deliberately post hostile and/or mocking messages in online discussion groups, message boards, or other social networking sites. Users will often “flame” back and forth, in the manner of a face-to-face argument (Hitchcock, 2002).

²“Mail bombing” occurs with a huge amount of the same email message is intentionally sent to an email address. The purpose of mail bombing is to overflow an email account’s inbox and cause it to shut down (Hitchcock, 2002).

³It was hoped that correlations between computer ownership versus computer lab use could be run to determine if one group was more likely to experiencing cyberstalking. But since the number of respondents who did not own computers was so small, a correlation would be meaningless.

⁴“Blog” is Internet shorthand for “web log”, online journals that are maintained by individual users. There are several blogging services available, including LiveJournal (<http://www.livejournal.com>), Xanga (<http://www.xanga.com>) and of course Blogger (<http://www.blogger.com/>). Users can also create blogs on their preexisting personal websites.

Table 1

Respondent Computer Use (n = 186)

Type of computer		Computer abilities		Take computer with them	
Desktop	41%	Expert	12%	Always	4%
Laptop/notebook	39%	Advanced	48%	Almost always	10%
Both desktop and laptop	19%	Moderate	38%	Sometimes	31%
Do not own a computer	1%	Beginner	2%	Almost never	16%
				Never	39%
Email frequency		AIM/IM frequency		Facebook frequency	
Do not use email	0%	Do not use IM	8%	Do not use FB	26%
3 times a day +	49%	Entire day	53%	Entire day	0%
2-3 times a day	35%	3 times a day +	5%	3 times a day +	7%
Once a day	13%	2-3 times a day	12%	2-3 times a day	13%
1-2 times a week	2%	Once a day	9%	Once a day	20%
Less than once a week	1%	1-2 times a week	7%	1-2 times a week	23%
		Less than once a week	5%	Less than once a week	12%
MySpace Frequency		Blog Frequency			
Do not use MS	57%	Do not use blog	80%		
Entire day	0%	Entire day	1%		
3 times a day +	2%	3 times a day +	2%		
2-3 times a day	4%	2-3 times a day	1%		
Once a day	9%	Once a day	1%		
1-2 times a week	14%	1-2 times a week	6%		
Less than once a week	14%	Less than once a week	9%		

Table 2

Respondent Demographics (n = 186)

Sex		Year standing		Residence	
Female	55%	Freshmen	8%	Dormitories	16%
Male	45%	Sophomore	12%	On-campus apartment	34%
		Junior	33%	Off-campus	50%
		Senior	45%		
		Graduate	2%		

Table 3

Respondent Internet Privacy Attitudes (n = 186)

The Internet makes it too easy to find people's personal information		It is not wrong to contact someone I don't know if they choose to make their information public		I would contact someone I had not previously met if I found their personal information online	
Strongly agree	21%	Strongly agree	4%	Strongly agree	3%
Agree	50%	Agree	30%	Agree	18%
Neutral	26%	Neutral	22%	Neutral	22%
Disagree	3%	Disagree	30%	Disagree	33%
Strongly disagree	0%	Strongly disagree	14%	Strongly disagree	24%

Table 4

Respondent Reports of Stalking Experiences (n = 186)

Type of Incident	Never (0)	Once (1)	Twice (2)	Three times or more (3+)	Not sure
I have received threatening letters through the postal mail	99%	1%	0%	0%	0%
I have received abusive letters through the postal mail	97%	2%	1%	0%	0%
I have had my reputation damaged rumors by that were spread by one or more individuals	70%	17%	8%	4%	1%
I have received threatening phone calls	86%	7%	4%	2%	1%
I have received abusive phone calls	83%	8%	2%	6%	1%
I have been followed during my daily routine	83%	8%	3%	2%	4%
I have been followed back to my home, apartment, or dorm room	86%	8%	2%	2%	2%
I have been confronted face-to-face by a person who followed me	90%	8%	1%	2%	0%
I have been physically attacked by a person who followed me	95%	4%	1%	0%	0%
I have felt in fear for my safety and well-being because of the incidents I've experienced	83%	9%	2%	5%	1%
I have changed parts of my daily routine because of the incidents I've experienced	90%	6%	2%	2%	0%
I have adopted personal security measures because of the incidents I've experienced	84%	8%	2%	5%	1%

Table 5

Respondent Reactions to Stalking Experiences (n =80)

Person responsible for stalking	How many stalking incidents were linked to same person		Currently experiencing stalking?		
Stranger	34% (22)	All	41% (31)	Yes	12% (9)
Former friend	20% (13)	Most	13% (10)	No	88% (67)
Friend	8% (5)	Some	13% (10)		
Classmate, coworker or acquaintance	21% (14)	A few	15% (11)		
Former significant other	14% (9)	None	18% (14)		
Current significant other	3% (2)				
Amount of time stalking occurred	Told stalker to stop?		How did respondent tell stalker to stop?		
Week or less	50% (38)	Yes	68% (52)	Sent a letter	9% (3)
1-4 weeks	18% (14)	No	32% (24)	Email	3% (1)
1 month-3 months	13% (10)			IM	10% (4)
3-6 months	9% (7)			Message on social networking website	0%
6 months or more	9% (7)			Phone call	18% (7)
				In person	58% (22)
				Asked someone to tell them	3% (1)
Stalking stopped after confronting stalker?	Reported stalking to Campus Safety?		Reported stalking to Women's Center?		
Yes	57% (29)	Yes	9% (7)	Yes	1%
No	43% (20)	No	91% (69)	No	99%

Table 6

Respondent Reports of Cyberstalking Experiences (n = 186)

Type of Incident	Never	Once	Twice	Three times or more	Not sure
I have received threatening e-mail	89%	6%	2%	2%	1%
I have received abusive email	85%	8%	4%	2%	1%
I have had threats made against me via AIM or another IM program	80%	8%	5%	5%	2%
I have had abusive comments made against me via AIM or another IM program	74%	11%	5%	8%	2%
I have had threats made against me in a chat room	93%	5%	1%	1%	0%
I have had abusive comments made against me in a chat room	94%	4%	1%	1%	0%
I have had threats made against me on a social networking website	95%	3%	1%	1%	0%
I have had abusive comments made against me on a social networking website	96%	2%	1%	1%	0%
I have had my reputation damaged by rumors that were posted online	89%	8%	1%	1%	1%
I have been impersonated online	87%	6%	2%	2%	3%
I have been "ganged up on" online by people who were encouraged to harass me	94%	2%	2%	1%	1%
Someone order goods or services online in my name without my knowledge or permission	95%	3%	1%	0%	1%
Someone intentionally sent me a computer virus (not junk mail/spam)	81%	8%	3%	4%	4%
I have been followed during my daily routine by someone who said they found my schedule online	96%	2%	1%	0%	1%
I have been followed back to my home, apartment, or dorm room by someone who said they found my address online	98%	1%	0%	0%	1%
I have felt in fear for my safety and well-being because of the incidents I've experienced	93%	5%	1%	1%	1%
I have changed parts of my daily routine because of the incidents I've experienced	95%	3%	1%	1%	0%
I have adopted personal security measures because of the incidents I've experienced	91%	6%	1%	2%	0%

Table 7

Respondent Reactions to Cyberstalking Experiences (n = 84)

Person responsible for cyberstalking	How many cyberstalking incidents were linked to same person		Currently experiencing cyberstalking?		
Stranger	33% (22)	All	37% (27)	Yes	12% (9)
Former friend	22% (15)	Most	20% (15)	No	88% (65)
Friend	10% (7)	Some	13% (10)		
Classmate, coworker or acquaintance	21% (14)	A few	4% (3)		
Former significant other	9% (6)	None	26% (19)		
Current significant other	5% (3)				
Amount of time cyberstalking occurred	Told cyberstalker to stop?		How did respondent tell cyberstalker to stop?		
Week or less	53% (39)	Yes	57% (42)	Sent a letter	0%
1-4 weeks	27% (20)	No	43% (32)	Email	11% (3)
1 month-3 months	10% (7)			IM	59% (16)
3-6 months	5% (4)			Message on social networking website	4% (1)
6 months or more	5% (4)			Phone call	7% (2)
				In person	15% (4)
				Asked someone to tell them	4% (1)
Cyberstalking stopped after confronting stalker?	Reported cyberstalking to Campus Safety?		Reported cyberstalking to Women's Center?		
Yes	60% (25)	Yes	1% (1)	Yes	0%
No	40% (17)	No	99% (72)	No	100%

Table 8

Computer Use for Respondents Who Experienced Cyberstalking Incidents (n = 84)

Type of computer		Computer abilities		Take computer with them	
Desktop	40%	Expert	15%	Always	4%
Laptop/notebook	37%	Advanced	45%	Almost always	14%
Both desktop and laptop	23%	Moderate	36%	Sometimes	35%
Do not own a computer	0%	Beginner	4%	Almost never	20%
				Never	27%
Email frequency		AIM/IM frequency		Facebook frequency	
Do not use email	0%	Do not use IM	8%	Do not use FB	25%
3 times a day +	54%	Entire day	56%	Entire day	0%
2-3 times a day	32%	3 times a day +	8%	3 times a day +	8%
Once a day	9%	2-3 times a day	13%	2-3 times a day	13%
1-2 times a week	4%	Once a day	6%	Once a day	19%
Less than once a week	1%	1-2 times a week	5%	1-2 times a week	23%
		Less than once a week	4%	Less than once a week	12%
MySpace Frequency		Blog Frequency			
Do not use MS	55%	Do not use blog	79%		
Entire day	0%	Entire day	2%		
3 times a day +	3%	3 times a day +	4%		
2-3 times a day	6%	2-3 times a day	2%		
Once a day	11%	Once a day	0%		
1-2 times a week	14%	1-2 times a week	8%		
Less than once a week	11%	Less than once a week	5%		