THE IMPACT OF COMPUTER MEDIATED COMMUNICATIONS ON STALKING SEVERITY: AN EXPLORATORY ANALYSIS OF CYBERSTALKING FIELD DATA

By

STEPHEN DEAN BARNES

Bachelor of Arts
University of Washington
Seattle, WA
1983

Master of Science in Telecommunications
University of Colorado, Boulder
Boulder, CO
1991

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
DOCTOR OF PHILOSOPHY
December, 2007

THE IMPACT OF COMPUTER MEDIATED

COMMUNICATIONS ON STALKING SEVERITY:

AN EXPLORATORY ANALYSIS OF

CYBERSTALKING FIELD DATA

Dissertation Approved:

Rick L. Wilson

Dissertation Adviser

David Biros

John Cross

Mark Weiser

A. Gordon Emslie

Dean of the Graduate College

ACKNOWLEDGMENTS

I would like to recognize a number of people who have supported this dissertation. Although I am listed as the only author, several people here have given unselfishly to enable this dissertation to be written. To all of them I owe a tremendous debt of gratitude.

First, to my chairman, Rick Wilson, thank you. Your efforts kept me on track and without your support, I would not have been able to complete all of the tasks assigned on this journey of discovery. Second, to David Biros, an even bigger thank you. Without your constant guidance and ideas, and most particularly your contacts at WHOA, I would not have had any data, or even such a topic to work with for this dissertation. I also owe thanks to Mark Weiser and John Cross for their support and contributions to this effort. This truly was a team effort.

Finally, my deepest thanks must go to my family. Thank you, Dad and Mom, for your constant support and encouragement. To my sons, Forrest and Ansel, thank you for understanding all the times when I could not play a family game, but rather had to be "up on the computer," working long hours at this dissertation. And last but most certainly not least, to Lani my wife, thank you. It was your constant harassment that started me down this road and kept me at it when I most wanted to walk away.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

ABSTRACT

The interaction between disjunctive interpersonal relationships, those where the parties disagree on the goals of the relationship, and the use of computer mediated communications (CMC) channels is a relatively unexplored domain. Bargh (2002) suggests that use of CMC channels can amplify the development of interpersonal relationships, and notes that the effect is not constant across communication activities. This dissertation reports on a line of research that explores the interaction between CMC and stalking, a common form of disjunctive relationship. CMC channels can be characterized by their richness, interactivity, and distribution (Te'eni 2001). Field data from cyberstalking cases is used to examine the effects of CMC channels on stalking case severity, and to explore the relative impacts of CMC channel characteristics on such cases. To accomplish this, a ratio-scaled measure of stalking case severity is developed for exploring the relationship between case severity and CMC media characteristics. This includes levels of anonymity, as well as the prior relationship between the stalker and the victim. Results show that channel richness and the nature of the prior relationship dominate the impact on cyberstalking case severity, while channel interactivity, distribution, and harasser anonymity do not affect case severity. In conclusion, this analysis of cyberstalking data provides support for Te'eni's (2001) CAMOC model and its interpretation of media richness theory. Further, the analysis provides evidence that disjunctive online relationships are different from disjunctive offline relationships only

when intimacy is involved. Follow-up research is proposed along with suggestions for the development of an improved measure of case severity.

CHAPTER I

INTRODUCTION

Research shows that the use of computer mediated communications (CMC) tools and techniques via the Internet can amplify and/or accelerate the development of interpersonal relationships (Bargh 2002; Bargh et al. 2002; McKenna et al. 2002; Hian et al. 2004), contrary to the expectations of early CMC and information systems researchers (Daft and Lengel 1986; Walther 1996; Dennis and Kinney 1998). Bargh postulates that this amplification occurs as the result of two main factors. First is the ability of individuals with common interests to find each other quickly and easily, even if widely separated geographically, using Internet search engines and chat rooms. This search capability accelerates the process of discovery of shared mutual interests, which are the foundation of stable relationships. Second, Bargh, McKenna and colleagues suggest that Internet CMC tools allow individuals to control the quality, quantity and type of personality they present online. This provides a means to diminish or temporarily remove personal characteristics (such as excessive weight) perceived to be detrimental to the initial development of a relationship, but that are more readily overlooked once a bond is formed (Bargh et al. 2002; McKenna et al. 2002). This process is shown to accelerate the disclosure of the desired persona and results in the strengthening of the relationship with the use of CMC tools (Bargh et al. 2002; McKenna et al. 2002).

In studying offline relationships, Cupach and Spitzberg (2004) introduce their book on obsession and stalking with the suggestion that interpersonal relationships take two potential forms. First, "when individuals pursue mutual activities and states, their shared relationship may be considered conjunctive in structure. Conversely, when relationships are nonmutual, they may be considered disjunctive in structure" (Cupach and Spitzberg 2004 p3).

Research on the longer-term impact of the effects of CMC on interpersonal relationships can explore either conjunctive or disjunctive relationships, or both, though most research to date has focused on conjunctive research. Only one study has addressed the nature of online stalking and online disjunctive relationships. Spitzberg and Hoobler (2002) explore cyberstalking, and conclude that it is different from offline stalking, but they fail to address the characteristics of cyberstalking in any depth. One line of research into CMC has shown that positive long-term effects on social interactions and psychological well-being among Internet users (Kraut et al. 2002) can also have worrisome consequences, through the reinforcement of "group think" phenomena as it occurs among extremist or anti-social groups (Glaser 1983; Spears et al. 2002). Additionally, CMC also allows people with extreme perspectives on any topic to find others of a like mind, leading to an amplified sense of support and reinforcement of such extremist views (Glaser et al. 2002).

In an organizational environment, Thompson and Nadler (2002) identify a negative impact from CMC on complex commercial negotiations where a greater understanding of not only the person, but the nuances of finer communication and the dynamic complexity of negotiation are required. While not completely disjunctive, such

negotiating relationships exhibit distrust and diverging ideas of the optimal outcome. This is the polar opposite to stalking, where a disjunctive relationship already exists and the communication of threat requires only baseline reading of the recipient's response. Many other forms of relationships are disjunctive, but as Cupach and Spitzberg observe, "…few seem so prototypical of disjunction as stalking and obsessive relational intrusion" (2004 p3). While much of the focus in past research on CMC is on relatively benign, conjunctive relationships, there are still substantial opportunities to research CMC usage and impacts in more disjunctive environments. For the purposes of this research, the focus will remain on disjunctive personal relationships.

Research Question

This leads to the following question: If the Internet and CMC tools can accelerate or amplify the development of conjunctive interpersonal relationships, what is its corresponding ability to amplify (or dampen) the impacts when a relationship is disjunctive in nature? While this is a broad question to answer, since there are a substantial number of reasons a relationship can be disjunctive (Cupach and Spitzberg 2004), this paper seeks to explore cyberstalking, a specific type of disjunctive relationship which may be influenced by CMC media effects.

One common outcome of the process of relationship dissolution is characterized by harassment of one person (commonly the person initiating the dissolution) by the other. Such harassment can take one of two common forms: obsessive relational intrusion (ORI, also known as hyperintimacy), in which the pursuer attempts to restore or strengthen the relationship, or stalking, where the pursuer is attempting to punish the

object of pursuit (Cupach and Spitzberg 1998, 2004). Cyberstalking uses Internet and CMC tools to accomplish ORI activities during the process of stalking. Understanding stalking and cyberstalking is of particular interest to wide variety of disciplines: academics, legal and clinical practitioners, and Internet service providers, all of whom must deal with the direct and side effects of ORI, stalking, and cyberstalking activities.

This paper first examines CMC processes associated with cyberstalking and the relative impact of CMC usage on cyberstalking victims, thus exploring one facet of the impact of CMC usage on disjunctive relationships. Secondly, it explores key characteristics of CMC channels and the impacts these independent characteristics have on cyberstalking cases.

Te'eni (2001) suggests three dimensions to communications media that may affect the medium's ability to convey stalking messages:

- interactivity (e.g. real time or delayed),
- richness (e.g. support for verbal communications),
- and type of distribution (e.g. typically private (peer-to-peer email) or public (blog)).

Additionally, CMC may provide the sender an effective form of anonymity, which may impact the cyberstalking victim in various ways. This research project began to explore these interactions using cyberstalking case histories, as a prelude to more focused future research on the topic.

Organization of the Paper

Chapter II introduces the reader to stalking and cyberstalking. It also identifies two dimensions of stalking. The first classifies stalking cases by the prior relationship between the stalker and the victim. The second identifies the location of the relationship, specifically if it an online or offline relationship. Types of online media used for stalking, as well as types of online and offline stalking actions taken, type of threat, and CMC moderator variables are also described. Chapter II also briefly reviews Te'eni's (2001) Cognitive-Affective Model of Communications and adapts the CMC channel characteristics identified by Te'eni into a trio of dimensions that can be easily identified and manipulated in an experiment. Chapter III develops a working model, and details the research hypotheses identified for testing with the available cyberstalking case data. Chapter IV introduces the cyberstalking case histories used in this research, and details the calculation of an index of case severity using the Analytic Hierarchy Process that was used as the dependant variable. A testing methodology is also described in this section. Chapter V presents the results, with indications of support for the hypothesis developed in Chapter III. Chapter VI is a discussion of the implication of this research for academic research and its value to the practitioner community. Included is a discussion on the limitations of this research activity and suggestions for future research, and the chapter ends with the conclusions drawn from this project.

CHAPTER II

BACKGROUND

Cyberstalking research sits squarely at the intersection of the research domains of sociology and computer mediated communications (CMC). Each of theses domains has a rich and deep background, but only recently has the full breadth of this intersection begun to be explored (Bargh 2002). Much of the existing research within this intersection deals with the positive, or normative, aspects of computer mediated communications (Bargh 2002; Cupach and Spitzberg 2004). This is reasonable, as it helps to first establish a baseline against which exceptions and disruptions may be compared. Cyberstalking is one such exception, capturing communications and harassing actions involving parties in disjunctive relationships. The research into cyberstalking reported here relies on knowledge of interpersonal communications processes, as well as the more personal aspects of relationship development and dissolution that flow from the sociological domain. It also requires a view of the information technology that influences not only the channel and form of communication, but also can intentionally or unintentionally distort or alter perceptions of the messages communicated between the sender and receiver of electronic transmissions (Te'eni 2001).

This chapter explores the existing research literature into both communications media as a communications channel and the impacts of communications as a vehicle for stalking and harassment associated with disjunctive interpersonal relationships. First, the

characteristics of communications media that may affect the impact of harassing messages are explored. Then harassment, stalking, and cyberstalking are introduced as they are currently understood in the research literature, leading to the specific hypotheses that are addressed by this paper, which are defined in Chapter III.

Cyberstalking as a Communicative Act

Reviewing the literature related to interpersonal communications, Te'eni (2001) assembled many elements of research around organizational and interpersonal communications into a comprehensive model of interpersonal and organizational communications that drew on media richness theory (Daft and Lengel 1986), the task-technology fit model (Zigurs and Buckland 1998), and a variety of other sources (e.g. Habermas 1984; Habermas and Cooke 1998; Straub and Karahanna 1998). Te'eni identifies this model as the cognitive-affective model for organizational communications (CAMOC) and develops a blueprint for its use in the development of technology in support of organizational needs.

A Cognitive-Affective Model of Organizational Communication

Te'eni's (2001) cognitive-affective model of organizational communications, or CAMOC, is useful as a lens for viewing the relationship between a stalker's goals, their strategy, the communications media, the message, and the outcome. Figure 1 presents Te'eni's CAMOC, which is briefly described and applied to stalking and cyberstalking in the following paragraphs.

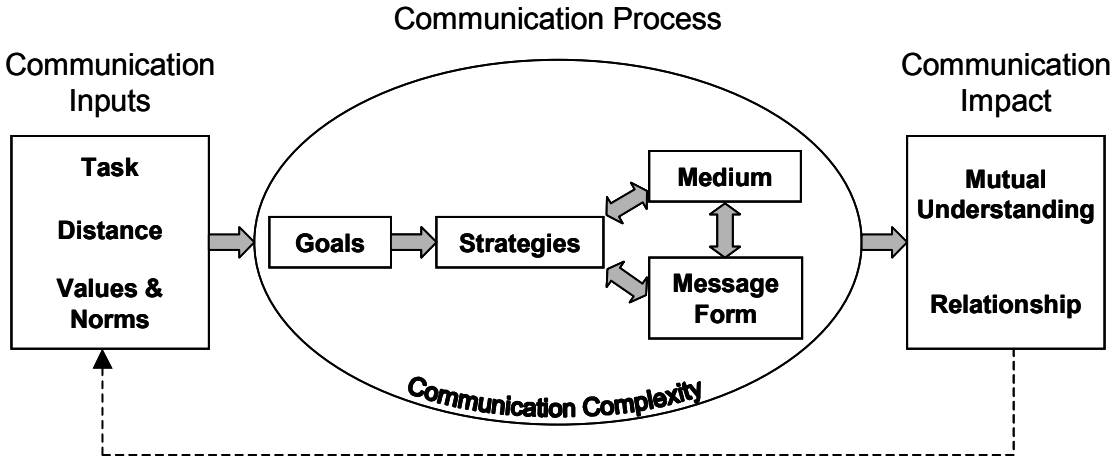


Figure 1: A Cognitive-Affective Model of Organizational Communication (adapted from Te'eni 2001 Figure 1)

While understanding the motivations of stalkers is beyond the scope of this work, such motivations include "… either deliberately or unconsciously, [to] seek control over their victim" (Finch 2001 p47). Conceptually, the social sciences have viewed affect (e.g. intimacy, love, affiliation, communion) and power (dominance, control, status) as both the primary axes of social life and generally orthogonal to each other (Birtchnell 1993). Cupach and Spitzberg extend this to stalking (and its common antecedent obsessive relational intrusion—both are defined later in this chapter), with power and affect providing motives, either independently or together, for either control over of the victim, or persuasive attempts to convince the victim that the stalker's perspective is honorable (Cupach and Spitzberg 2004 p57). Other research indicates that almost half of all stalkers are individuals seeking to persuade a former intimate partner to return to the relationship, or failing that, to punish the victim for not responding to the stalkers overtures (Zona et al. 1993; Pathe and Mullen 1997; Meloy 1998; Mullen et al. 1999; Tjaden and Thoennes 2000; Sheridan et al. 2001a; Cupach and Spitzberg 2004). Most other stalkers have a

similar goal, but begin with a different relationship to the victim (Tjaden and Thoennes 1998; Sheridan et al. 2001b; Spitzberg and Hoobler 2002).

Punishment (or control, since both represent the use of power) and persuasion (representing affect) thus become task inputs into the communications process under study here (see Figure 1). Te'eni's identifies two dimensions for the second input, cognitive distance (differences in knowledge or understanding of the topic), and affective distance (the emotional gap), each of which represents a difference between the state of the stalker, or sender, and the state of the victim, or receiver. Te'eni's third input, values and norms, represents cultural knowledge that guide behavior related to communications within that culture (Te'eni 2001 p257). This trio of inputs collectively affects the various elements of the communications process used to deliver the senders message(s) to the receiver.

Within the communications process, the goal associated with each message is related to the impact desired. Te'eni (2001) addresses the organizational context with the CAMOC, but as Cupach and Spitzberg note

> "Most existing theory and research on relational and interpersonal competence propose skills such as message management, coorientation, and adaptability *for the purpose of engendering mutual respect and sustenance of ongoing dialogue*. Yet mutual respect and sustenance of dialogue are often precisely the objectives the unwanted pursuer seeks to impose on the victim, and precisely what the victim seeks to deny the stalker." (Cupach and Spitzberg 2004 p157, emphasis in original).

Thus Te'eni's CAMOC must be validated for use with disjunctive relationships before such relationships can be used to address questions associated with the communications process. Such use is foreseen by Te'eni, who states "The criterion for choosing the landmarks for the central path [through the model] concerns how to best uncover the

process of communication so that others can forge new paths along similar lines for new conditions." (Te'eni 2001 p256).

Validating CAMOC With Respect to Disjunctive Relationships

The CAMOC is a two layer model, consisting of inputs, impacts (outputs), and a channel (the communications process) between the sender and receiver, as shown in Figure 1. Initial validation requires that the inputs and outputs be compatible with the model. If the higher layer of inputs and outputs are compatible, then no changes are needed to the lower communications process layer when the communications processes are used in support of communications associated with a disjunctive relationship.

To validate the inputs and outputs requires that one first understand the assumptions that underlie the CAMOC. Taking the outputs first, begin with the fact that Te'eni based the CAMOC on Habermas's theory of communicative action (Habermas 1984; Habermas and Cooke 1998; Te'eni 2001). The theory of communicative action provides a notion of successful communications between humans (Habermas 1984). Habermas (1984) claims that four conditions are necessary for a communicative act to take place:

- the act must be comprehensible, so that the receiver can understand the sender;
- the act must be true, so that the receiver can share the sender's knowledge;
- intentions must be expressed truthfully, so that the receiver can trust the sender; and
- the act must be appropriate within some normative context so that the receiver can agree with the sender within this value system. (Habermas 1984)

As noted by Cupach and Spitzberg, the scientific literature is generally in agreement with Habermas (Cupach and Spitzberg 2004, see quote above). Successful communications generally follows a positive norm, wherein both parties to the communicative act increase their mutual understanding and improve the relationship (Habermas 1984; Te'eni 2001 p261). The inverse is also accepted, since IS researchers commonly characterizes impediments to action and relationship as poor communications (Te'eni 2001). This aligns with Cupach and Spitzberg's (2004) notion of conjunctive relationships. For this study of disjunctive relationships, this definition of communications success must be modified in two areas.

First, note that in terms of a communications channel, the direction of the cognitive-affective impact does not matter, but the magnitude does. That is to say, there is a difference between size and direction. The channel can reduce the ability to convey meaning if it does not have sufficient capacity. However, a given channel can carry information damaging to a relationship of a given cognitive or affective magnitude just as easily as it can carry information conducive to the relationship at the same cognitive or affective magnitude. For this reason, *the magnitude of the impact is more significant than the direction* (e.g. positive or negative) of the impact when studying a communications channel. Applying this in the context of harassment, a harassing message will increase mutual understanding, while also causing a strong, negative affective response within the receiver, leading to a decrease in trust and injury to the relationship (Sheridan et al. 2001a). Given that some stalkers seek to harass or injure, we must accept that, from the senders perspective, a harassing message leading to a negative affective impact on the receiver is successful. However important the victim's view, for the purpose of this

research it is necessary to approach this from the stalker's perspective, since it is the sender-stalker that makes the choices about channel and message. Thus for the purposes of this study, the definition of success of the communicative act must carefully be constrained to mean a change of affect, without concern for the direction of the change. We conclude then that the more severe the impact on the victim, the more effective the communications channel was in transmitting the intended message from stalker to victim.

The second change associated with communications success addresses Te'eni's notion of cultural norms and values (Te'eni 2001). Returning to CAMOC's inputs, note first that persuasion is one of the core functions (goals) of the communicative act (Habermas 1984; Habermas and Cooke 1998; Te'eni 2001), and is a direct goal of many stalkers (Sheridan et al. 2001b; Spitzberg 2002). Thus a stalker message motivated by a need to influence or persuade the victim is clearly compatible with the CAMOC as a task input, but will fail to achieve the impact intended by the stalker due to its incompatibility with cultural norms and values as accepted by the receiver-victim. Alternatively, a stalker may be motivated by a need to punish the victim. This is harder to reconcile with the CAMOC, as the CAMOC assumes that all participants agree on a group goal at some higher level, and that the intent of any communications is to enable action towards such a goal. Fundamentally, stalkers and their victims fail to share a common goal. However, victims will generally agree that a negative message is harmful, which implies agreement with the harasser at one level, if the harasser's message is intended to punish. In this case, the stalkers message is successful, even though it violates cultural norms and values against harassment and negative messages.

This leads to the conclusion that a violation of cultural norms and values does not necessarily invalidate the senders perception of (or the actual) success when the intent is (consciously or subconsciously) to violate cultural norms and values. Thus the second change to the definition of communications success needed is that when addressing communications between parties in disjunctive relationships, such communications will often violate cultural norms and values. Such a violation may be intended by the sender, and if intended, has the potential to amplify the impact of the message, leading to successful communication from the perspective of the sender.

Most importantly, a violation of cultural norms and values associated with the generation of a message stream's content does not necessarily affect the communications processes associated with delivering that message stream across some communications channel to the receiver. An example may be useful here. Consider the common management nostrum of praise in public, discipline in private, taken here at face value as a cultural norm. If a manager disciplines someone in public, the action either adds significance to the discipline by making it public (implying a more significant infraction), or it demonstrates the manager's inability to adhere to a cultural value. The difference between the two alternatives is determined by the true significance of the infraction, and any formal rules associated with the discipline process (cultural norms again). Neither alternative has any impact on the communications process once one is chosen by the manager, and both cases use a communications process to effectively communicate with the recipient(s).

Development of a proof that violations of cultural norms and values will fail to affect the communications process is beyond the scope of this paper, and may be

practically impossible. Since it is possible that violations do not affect the communications process, as shown by the preceding example, the assumption is made that such violations are not harmful to the communications process under study, and thus that punishing messages sent by a stalker or harasser can be effectively delivered by the communications process outline in Te'eni's (2001) CAMOC.

The next section briefly describes these communications processes, and defines three characteristics of media that are tested in this project for their impact on stalking case severity.

Communications Processes

Referring again to Figure 1 showing Te'eni's (2001) CAMOC, the inner layer addresses the communications processes. First, message goals are derived from the sender's motivation as captured in the inputs for task, distance, norms, and values associated with the communications. Message strategies, media choices, and message forms are chosen by the sender to serve that goal, and will reflect the inherent limitations of these elements. For example, an asynchronous medium will not be used in supporting a task requiring high levels of interaction and dialog. Assuming that the sender (and receiver) has a modicum of experience with the available media, types of message forms, and necessary strategies, such experience will enable effective translation of the message goal into an appropriate set of media and message form choices (Te'eni 2001).

Implicit in this process is an understanding of the limitations of the media used, with the limitations characterized in multiple dimensions. Te'eni suggests three characteristic dimensions of channels that are likely affect the senders choice of medium (relative to some intended strategy): channel capacity, interactivity, and adaptiveness

(Te'eni 2001 p271). Channel capacity in this context is not the raw bit rate, but rather the ability of the channel to support a variety of verbal and non-verbal cues and hints that a perceptive receiver can use to interpret the message content (Te'eni 2001 p271; Kock 2004), and is often known as channel or media richness. Interactivity relates to the ability of the channel to support real time dialog between the parties (Te'eni 2001). Finally, adaptiveness in Te'eni's (2001) terms is the ability of a medium to tailor a message for a given recipient. Thus, blogs and bulletin boards are less adaptive than personal email. Te'eni cites only one study of adaptiveness, Adams et al. (1993), suggesting a paucity of research in this area. The following paragraphs examine these characteristics in more detail.

Media richness has long been suggested as a characteristic of a communications channel that affects the ability of that channel to support messages with varying levels of cogitative and affective content (Daft and Lengel 1986; Carlson 1995; Zigurs and Buckland 1998). More recent research has failed to support the full breadth of the original media richness theory (Dennis and Kinney 1998; Dennis et al. 1999). However, Kock (2004) divides media types into two groups, those that support natural speech (face-to-face, video, phone) and those that do not (i.e. text-based), thus limiting the scope of the richness dimension. This research uses Kock's definition of richness, dividing the existing media technologies into verbal and textual media, and uses cyberstalking case information to test the effects of richness on case severity.

Interactivity, or the delay imposed on a message as it transits the media, captures the difference between real time or synchronous communications and delayed or asynchronous communications. Te'eni identifies it as "the potential for immediate

feedback from the receiver" (Te'eni 2001 p271), and suggests that higher levels of interactivity facilitates control through testing and adjustment as a response to instant feedback. Such dynamic controls are necessary in situations that exhibit high levels of dynamic complexity (McLaughlin 1984). Further, interactivity requires that the participant be able to respond "on the fly" to an unpredictable progression in the dialog, making it more difficult, and potentially a liability to the sender (Te'eni 2001). This research sorts media into two categories of interactivity, real time and delayed, and tests the impacts of this division on cyberstalking case severity, as described below in Chapter III.

Te'eni suggests that adaptiveness is necessary when the strategy of the sender requires that the message be tailored for a particular recipient, and that some communications media are more adaptable than others. Channels with higher levels of adaptiveness should be more attractive to stalkers who are seeking to address their messages to a particular victim. While not identical, the message distribution mechanism used by a media can be seen as a proxy for Te'eni's adaptiveness construct (Te'eni 2001 p274). Distribution mechanisms can take on a similar role, by providing control to the sender over how and when the recipient receives a message. Distribution mechanisms can be divided into two subgroups, private and public, that can also be thought of as sender-driven and recipient-driven, respectively. Private distribution mechanisms, such as the telephone and email, are controlled by the sender, who chooses the recipient of the message. Recipients of publicly distributed communications are not controlled by the sender. Rather, the sender posts the message in a public place, and anyone is welcome to read (or listen to) it. In practice, recipients will choose to "subscribe" to a public channel,

and then choose (or not) to read each message posted there. Public distribution is typified by broadcast radio, newspapers, websites, and blogs. This division captures the difference between CMC media that are effectively private (or peer-to-peer), with the sender specifically identifying the recipients, and those that are distributed more widely (e.g. to the public), with the recipient choosing to subscribe to the channel and further choosing to read (or listen to) each message or not. This research tests the difference in impacts on cyberstalking case severity associated with the use of public and private distribution mechanisms used by various media.

Channel Characteristics of CMC Tools

Table 1 shows the association of a variety of current CMC tools, organized with these three channel characteristics of richness, interactivity, and distribution. Note that there are no known applications that fit the public verbal interactive category, although one colleague argued that a "Boston Commons" type public space would qualify if it existed today. In a limitation of this research, the data used for this project (discussed in Chapter IV) does not contain any cases that specifically identify the public verbal delayed category, and only two cases that mention voice mail in the private verbal delayed category, thus effectively constraining this research to the remaining five categories shown.

Table 1: CMC Channel Characteristic Map

	Richness: Verbal		Richness: Text	
Interactivity:	**Real Time**	**Delayed**	**Real Time**	**Delayed**
Distribution: Private	FTF, Phone, Video Conf, Webcam	Voice Mail	IM, ICQ, (Hacking?)	Email, SMS, Postal Mail, Ecards
Distribution: Public	None Known	Broadcasting, Movies, YouTube	Chat, Game Forums	Blogs, Lists, Msg. Boards, Websites, Ebay ratings, Usenet, Wiki Entries

In summary, this section has shown that disjunctive relationships generating harassing cyberstalking activities and messages violate only the cultural norms and values inputs associated with use of communications processes, and that such violations are associated with the direction of the impact. Specifically, cultural norms assume that successful communications will decrease the cognitive and/or affective distance between the parties, and that higher levels of change are good. In disjunctive communications associated with punishment, the impact will increase the cognitive and/or affective distance between the parties, violating the assumed cultural norm. Having no evidence to the contrary, and noting that proof is beyond the scope of this paper, the assumption is made that such a change in the direction of cognitive or affective impact on the victim has no impact on the functioning of the communications process used to support the message. Thus stalking cases can provide us with tests of the ability of communications media to affect disjunctive relationships, which are more fully detailed in the next section.

Stalking, Cyberstalking, and Online Harassment

The academic literature generally defines stalking as "a series of actions directed at one individual by another that taken as a whole amount to unwanted persistent personal harassment" (Sheridan et al. 2001b p152). Goode (1995) suggests that stalking is a pattern or "course of conduct" of intentional harassment intended to cause emotional distress. Obsessive relational intrusion (ORI), which is closely related to stalking, consists of excessive efforts on the part of the perpetrator to develop a relationship with a victim, often to the extent that normally positive acts take on negative connotations in the perception of the victim (Sheridan et al. 2001a; Cupach and Spitzberg 2004). A common working definition encompasses stalking and ORI (along with persistent harassment not originating from a close relationship), as it is the perception of the victim that legally determines if harassment is taking place (Cupach and Spitzberg 1998, 2004). Further, since even relatively mild efforts at such courtship often cross the threshold of threat and fear by virtue of their repetition (Cupach and Spitzberg 2000), and the fact that ORI can easily morph into stalking, it is very likely that some cases labeled stalking are actually cases of ORI (Emerson et al. 1998). Since the differences between ORI and stalking are only minimally important for the purposes of this study (Harmon et al. 1995), which approaches the topic from the victim's perspective and avoids direct analysis of the perpetrators motive, this paper will use a somewhat relaxed definition of the term *stalking*, which includes both "classic," or criminal, stalking and more aggressive forms of ORI, unless otherwise noted.

Cyberstalking is stalking perpetrated exclusively or largely with computer mediated communications (CMC) and/or a wide variety of other online applications and

services (Spitzberg and Hoobler 2002).[1] CMC can provide support for offline stalkers, as a tool in their kit (Spitzberg and Hoobler 2002), or a cyberstalker can operate purely online, even when the victim is not a regular user of the Internet. The former includes the example of a stalker using the Internet to collect information about an offline victim. The latter is demonstrated in the case of Gary S. Dellapenta, who severely traumatized his victim via personal ads placed on the Internet (Miller 1999b). Cyberstalking has recently become a recognized phenomena (Miceli et al. 2001; D'Ovidio and Doyle 2003), but there have been only a few pilot studies of its prevalence and impacts on victims (Spitzberg and Hoobler 2002; Finn 2004; Alexy et al. 2005).

There appears to a shortage of studies that attempt to characterize cyberstalking by the methods and media used by the cyberstalker, or how use of those methods correlated to their impacts on the severity of the case. Thus, one focus of the first part of the larger research program is on the CMC choices of cyberstalkers and the resulting impacts on their victims. This is accomplished using 1150 cyberstalking case histories from a victim's advocacy group that include a wide variety of CMC tools and techniques that go well beyond the ubiquitous email and instant messaging services that are commonly included in research into CMC. These case histories will be discussed in greater detail in Chapter IV of this manuscript.

As a practical matter, this paper will separate serious stalking from lesser forms of conflict with stalking defined to be continued threats or harassing actions by the stalker after clearly being told to stop at least once. This paper adopts this definition as the working definition of cyberstalking, since it is the one used by the victim's advocacy

[1] In practice the term cyberstalking also encompasses some cases better classified as online incidents of ORI.

group, Working to Halt Online Abuse (WHOA 2006). Note that this definition includes some "school yard bullying" and other forms of minor harassment, and is not limited to formerly intimate relationships. However, it does not generally include workplace or sexual harassment that is merely denigrating to the object of the harassment, due to the generally transient nature of such harassment, and the lack of any implied or explicit threat to the victim.

Rosenfeld (2004) suggests some caution in the use of the terms stalker and victim:

> Regardless of whether researchers have chosen to label their subjects as stalkers, obsessional followers, obsessional harassers, or erotomanics, most have essentially targeted the same offender population. Hence, for the sake of consistency, the term stalker is used here with the caveat that many of these individuals have not actually stalked (i.e., followed in a stealthy manner) their victim(s). It should also be noted that the use of the term victim in reference to the target of stalking is also somewhat controversial, with many writers preferring the term survivor (despite the unfortunate fact that not all victims survive the stalking experience) or target. Despite this controversy, the term victim is retained here with the acknowledgment that no negative connotations are intended by the use of the term (Rosenfeld 2004 p10).

This paper adopts Rosenfeld's terms and respective definitions for "stalker" and "victim." Further, this paper uses "harasser" and "perpetrator" as synonymous with "stalker."

Dimensions of Stalking

While stalking is an old phenomenon, understanding it is has become the focus of research efforts only since the mid 1990s. More recently, it is becoming clear that classifying stalking and its less severe antecedents, harassment, bullying, hyperintimacy, and obsessive relational intrusion (Cupach and Spitzberg 1998), requires several dimensions. These include the context (e.g. personal or work, online or offline) and nature of the relationship and its origin (Harmon et al. 1995), the nature of the attachment

between the perpetrator and victim (e.g. conjunctive or disjunctive, Zona et al. 1993; Harmon et al. 1995; Cupach and Spitzberg 2004), and the form or severity of the harassment (Cupach and Spitzberg 1998; Sheridan et al. 2001b; Spitzberg 2002). Less clear is the time dimension. Some forms of harassment are shorter in nature, and one study found a distinct difference between incidents lasting less than two weeks and those lasting longer (Purcell et al. 2004). These dimensions are discussed in the following paragraphs.

The Relationship Intimacy Level

Initiating an interpersonal relationship is difficult. Ending an intimate relationship is nearly always more difficult, and invariably results in pain to both parties (Heinlein 1966 p259-60). Emerson et al. (1998) suggest that stalking is most likely to originate as a relationship begins or ends, and that most cases of stalking are a dynamic process that evolve from a normal relationship through hyperintimacy (or ORI) into classic stalking. This is supported by the evidence, which suggests that upwards of 50% of classic stalking cases resulted from the dissolution of some form of intimate relationship, either as spouses, sexual partners, or a dating relationships that lasted more than a few weeks (Tjaden and Thoennes 1998, 2000; Spitzberg 2002). Emerson et al. (1998) extensively explore the qualitative nature of the development of the ongoing relationship between the stalker and the victim over time, and note that most incidents of stalking begin innocuously, and that most victims only recognize it as stalking retrospectively.

With respect to stalking associated with domestic violence, a variety of researchers have developed typologies of stalking relationships (e.g. Zona et al. 1993; Goode 1995; Spitzberg and Cupach 1998; Sheridan et al. 2001b; Spitzberg and Hoobler

2002; Mohandie et al. 2006; Roberts and Dziegielewski 2006). Sheridan et al. (2001a) captures a concise typology, providing for five main categories:

- Domestic violence stalking by a current or former intimate partner.
- Domestic violence stalking by another family member.
- Stalking by friends/acquaintances.
- Stalking by strangers/erotomanics.
- Stalking by unknown or anonymous stalkers.

This paper uses Sheridan's typology to characterize the relationships between stalker and victim in this research, with a further extension representing the context in which the relationship began.

The Context of the Relationship

This dimension is intended to capture the context of the relationship, in the sense of where the stalker meets and interacts with the victim. Traditionally, this meant interaction at work, at school, in some public place, or at a social event of some nature. For this study, the context of interest is "online" or "offline," thus characterizing the relationship as purely online, or one that exists offline and uses online tools for communications.

Today, some of the most popular web sites on the Internet are social networking sites, some of which are explicitly designed to facilitate the process of initiating relationships. McKenna et al. (2002) reported on the history and evolution of such online relationships, and the progression from email and Internet relay chat (IRC) to conversation over the telephone to meeting in person. This research has produced a variety of interesting results. Bargh et al. (2002) and McKenna et al. (2002) together

show that use of CMC allows individuals to more easily present their "true selves" and, on the receiving side, map that to the receiver's ideal of the person presented. This accelerates the formation of relationships, and often leads to long-term friendships and offline intimacy (McKenna et al. 2002). Supporting this conclusion, Hian et al. (2004) demonstrated that contrary to expectations, CMC actually accelerated the development of relations over face-to-face communications in zero-history dyads in a organizational environment. They base their work on the hyperpersonal communications model proposed by Walther (1996).

This leads to the question of how the Internet affects the harassment acts of stalkers. Clearly, some harassing acts translate easily into the online realm, such as use of email or other forms of messaging to propose dates, etc. Similarly, verbal and written threats can easily be transmitted using CMC tools. Conversely, direct physical aggression is not possible online. In the middle, there is considerable scope for the misuse of information systems with the aim of harassing a victim. Forms of such harassment can include but are not limited to impersonation of the victim, identity theft leading to fraudulent use of same, theft or misuse of intellectual property, and various forms of reputational harassment and slander. As the present research activity directly involves the difference between online and offline relationships and communications channels, this context dimension represents a key construct in the model developed in the next chapter.

Anonymous Stalkers

Unknown or anonymous stalkers represent a special case of the relationship and context dimensions. While relatively rare in the classic stalking literature (Sheridan et al. 2001b; Cupach and Spitzberg 2004), CMC tools provide an easy means for a cyberstalker

to remain anonymous to unsophisticated users and some ability to remain hidden from even the most sophisticated of network experts in practice (Berthold et al. 2000). Only a few studies clearly distinguished between stalking by strangers and anonymous stalkers (e.g. Sheridan et al. 2001b; Spitzberg 2002). These are not necessarily the same thing. Strangers are individuals otherwise unknown to the victim at the onset of the stalking activity, but who do not necessarily try to hide their identity. Anonymous stalkers hide their identity, and may be strangers, but may also be friends, acquaintances, family members, or former intimates known to the victim, but that are not known to be the stalker, even after a substantial number of harassing acts have occurred.

The use of anonymity as a construct has a long history in group support system research showing that use of anonymous communications can impact the willingness of a subject to communicate, and that it can change the content of the message sent (Connolly et al. 1990; Zigurs and Buckland 1998; Dennis et al. 2001). Theoretically, this is based on the removal of potential negative consequences to the sender (Connolly et al. 1990; Dennis et al. 2001). A desire for anonymity on the part of a stalker will likely influence the choice of communications media, eliminating the richest media since face-to-face contact and, to a lesser extent, voice contact via telephone do not generally allow the stalker to remain anonymous. Maintaining anonymity can also be seen as a goal that limits a stalker's communications strategy choices within Te'eni's (2001) model of interpersonal communications processes.

The Form of Attachment

With respect to the third dimension, attachment, Harmon et al. (1995) note that the form of attachment between the stalker and victim can take on one of two aspects:

first, an affectionate or amorous attraction, where the stalker is attempting to win over the victim, but is being rebuffed by the victim, and second, a persecutory or angry attachment, where the aim of the activity is punishment for some perceived wrong. Several researchers note that the practical differences between these aspects is smaller than it first appears (Harmon et al. 1995; Cupach and Spitzberg 1998; McCann 2001; Cupach and Spitzberg 2004). Emerson et al. (1998) note that the shift from ORI to stalking consistently occurs late in the typical evolution of a stalker/victim relationship, and is marked by the realization on the part of the stalker that their overtures have failed. Further, it is often only at this point in the relationship that the victim will label the efforts of the perpetrator as stalking, and that the stalker and victim agree on the nature of the relationship (ergo, that it is classic stalking) (Emerson et al. 1998).

There has been significant research into how the motivation of stalkers differs from that of non-stalkers, and the related development of clinical psychopathologies of stalkers. As this is beyond the scope of the present research, the interested reader is referred to Cupach and Spitzberg (2004) for a review of recent research in this area. Research to date provides no evidence that use of CMC tools affects the motivations of stalkers, or that the form of attachment varies between classic offline stalkers and cyberstalkers. Similarly, there is no evidence of any differences in the motivation of ORI perpetrators operating online or offline (Spitzberg and Hoobler 2002).

Temporal Dimension

There are two time dimensions in stalking. First is the evolution of the stalking process within a given case, as noted above. Both Emerson et al. (1998) and Cupach and Spitzberg (2004) address this in some detail, noting that what is known is less than ideal,

since it has not been possible to observe cases in a true longitudinal fashion. It is only in the latter stages of the process that the parties and observers typically identify the case as stalking. Further, these same authors note that classic stalking is often episodic, with specific events marking the progression of the case.

The second time dimension represents the duration of the case. Cupach and Spitzberg (2004) also address this dimension, reviewing 43 prior studies that collected data on the duration of stalking cases. Definitional differences confound their analysis, but their meta-analysis indicates that typical stalking cases last around 22 months (calculated as the mean of reported central tendency data). For example, Sheridan et al. (2001a) analyzed 95 cases handled at a victim's support clinic in the UK, and found that 14% ended in less than a year, only 29% had ended at the time of the survey, and that 14% were still active 10 years after the initiation of stalking activities. One case had been active for more than 43 years.

It appears that duration is a good indicator of the nature of the harassment. Purcell et al. (2004) used a large sample survey to test for differences in the impacts of shorter or longer stalking incidents, and found a significant break at 2 weeks. They found that psychological damage to the victim was more severe for cases longer than 2 weeks, a finding echoed by Mullen et al. (2000). Purcell et al. (2004) reported that short incidents (45% of stalking incidents) generally involved strangers (75.5%), averaged only 2 days in duration, and the median number of harassing acts ("intrusions") reported by this group was five (range: 2 – 40). Long incidents generally involved stalkers known to the victim (82.5% overall, 21.4% were former intimates, 30.3% were acquaintances, 22.2% were from a work context, and 8.5% were estranged family or friends), and involved more

harassing acts (median of 20, range 8 – 85). The median duration for long incidents was 6 months, with a modal length of 12 months. Purcell et al. (2004) conclude by noting that the 2 week time frame is sufficient to demonstrate that the perpetrator's behavior is purposeful, and will likely lead to a much longer and more severe incident.

Harassing Acts

Legal definitions of stalking all center around a pattern of "persistent personal harassment" (Sheridan et al. 2001b p152) whereby the individual acts may or may not, in themselves, be considered harassment. They concluded that, like fine art, stalking is easy to spot but hard to characterize. Such harassment can cover a very broad range of acts and often does so even during the progress of a single case of stalking. Spitzberg (2002), in a significant meta-analysis, developed a typology of stalking based on the actions of stalkers found in his literature review. Spitzberg grouped the actions into seven categories of roughly increasing severity, as defined in Table 2, and suggests that this set of categories can become a framework for the development of measurement schemes of stalking activity (Spitzberg 2002 p272). This paper uses Spitzberg's categories as the basis for a case severity index, as described further in Chapter IV.

Table 2: Typology of Stalker Actions (Spitzberg 2002)

I.	Hyperintimacy	Expressions of affection; Excessive courtship behaviors; Excessive communications attempts; many unwanted gifts.
II.	Pursuit, Proximity, & Surveillance	Lying in wait; Synchronizing activities; Unauthorized photos; Following; Drive-bys.
III.	Invasion, Theft, Vandalism	Violation of legitimate privacy; Invasion; Information theft; Property theft or damage.
IV.	Proxy Pursuit & Intrusion	Involve third parties for information gathering or proximity opportunities; Intimidate via intermediaries.
V.	Intimidation, Slander, & False Charges	Threats; Sabotage and Reputational Harassment; Blackmail; Threats of disclosure to employer; Making false claims to social services.
VI.	Coercion & Constraint	Forceful limiting of victim's options or behaviors; Extortion; Use of physical force; Kidnapping.
VII.	Aggression	Assault on property, pets, self, or others; Violence towards victim; Rape; Endangerment.

With respect to online harassment, Spitzberg listed calls, electronic contacts, and notes/messages/photos sent under hyperintimacy, information theft under invasion, and verbal or written harassment under the intimidation category (Spitzberg 2002). Hacking and impersonation online were not included in Spitzberg's typology details. Note that online tools provide excellent capabilities for indirect harassment of a victim. For example, the placement of a false profile on a social networking site with the victim's contact information can lead to a deluge of messages directed at the victim. On its face, this shows the flexibility that online techniques can have in supporting harassment and stalking activities.

Note here that online technologies are tools not strategies, and can be used to support harassment acts that fall into any of the first five of Spitzberg's strategies as listed in Table 2.

Online Methods Used by Cyberstalkers

A number of authors have noted that cyberspace provides stalkers with new tools that allow them to stalk the victim anonymously and/or by proxy (D'Ovidio and Doyle 2003; Bocij 2004; Aggarwal et al. 2005; Alexy et al. 2005; Beran and Qing 2005). In one early study, Fisher, Cullen et al. (2000) found that email was used in 25% of traditional stalking incidents identified in a randomly selected national survey of 4,446 women who were attending a 2- or 4-year college or university during the Fall of 1996.

A search of the literature found only two studies that attempted to determine the prevalence of particular online tools. Using data from the New York Police Department Computer Investigation & Technology Unit (CITU), one study found that email was the most common technology, used in 79% of cases, with instant messaging (IM) following in 13% of cases. Other methods used included chat groups (8%), message boards (4%), web sites (2%), with news groups and fake profiles appearing in only 1% of cases (D'Ovidio and Doyle 2003). 92% of cases used only one CMC method. The D'Ovidio and Doyle study, based on police records, is unable to report on incidents not reported to law enforcement, and thus leaves a significant gap in the research. Researchers in the second study found that 16.2% of students on a college campus had received harassing emails, 19.3% had received harassing IM messages, and 14.1% reported that the email harassment did not stop when requested. Similarly, 13.1% reported that the IM harassment did not stop when requested (Finn 2004). Most students in this survey did not report using chat, news groups, or other online technologies. Given the limited research into methods used by cyberstalkers, especially outside of the campus environment, this calls for further exploration of harassment methods in the CMC environment.

Case Severity in Cyberstalking

The best measure of the severity of a stalking case is the psychological impact on the victim (Goldberg et al. 1997; Purcell et al. 2004). Data for this is not readily available without an extensive data collection process, so a proxy for this measure is required. Purcell et al. (2004) show a significant connection between the frequency and number of harassing acts, threats, and aggression and the resulting psychological impact on the victim. Purcell and colleagues showed that stalking cases lasting longer than two weeks had elevated measures of psychological morbidity and were more severe in all categories than stalking cases lasting less than two weeks. Their measures were the 28-item General Health Questionnaire (Goldberg and Hillier 1979), a screening measure of current general psychiatric morbidity, and the Impact of Event Scale (Horowitz et al. 1979), a measure of post-traumatic stress reactions associated with victimization. Further comparison of both morbidity measures between short cases and non-stalking survey respondents were not significantly different (Purcell et al. 2004). This leads to the conclusion that increases in duration, action frequency, threat volume, and aggression can be associated with increases in psychological impacts on the victims. This research activity utilizes Purcell's conclusions to develop an index of case severity, which is based on the presence (or not) of various actions and threats in the case record, and which is used as a proxy for measures of psychological morbidity. The details of this approach are provided in Chapter IV.

Because stalking (and cyberstalking) are made up of many smaller actions, there has been an ongoing debate in the legal and practitioner communities about what constitutes the crime of stalking, and this is reflected in the research literature (see, for

example, Dziegielewski and Roberts 1995; Goode 1995; Ellison and Akdeniz 1998; Tjaden and Thoennes 1998; Sheridan et al. 2001b; Sheridan et al. 2002; Brenner 2004; Phillips et al. 2004; Roberts and Dziegielewski 2006). Each of these papers attempts to answer the question of whether particular types of incidents are serious enough to be labeled a crime. Unfortunately, these works assume a binary outcome, crime or not, and do not measure or propose measures of the degree of impact on the victim.

CHAPTER III

RESEARCH MODEL & HYPOTHESIS

Research Model

The formal research model explored in this paper is shown below in Figure 2, and consists of two main elements. The first element addresses the interaction of the type and intensity of the prior relationship between the stalker and the victim, and the context in which the relationship existed, where the latter is divided into online and offline relationships. This interaction is the subject of the first hypothesis under study (H1 in Figure 2), and underlies all of the following work. A series of additional hypotheses extend the analysis of this interaction to look into postulated differences related to intimacy level (H2) and anonymity (H4) on the part of the stalker. The second element attempts to explore a trio of the various characteristics of computer mediated communications that may have an impact on cyberstalking. This trio of characteristics includes media channel richness (H5), interactivity (H6), and distribution (H7), as identified by Te'eni (2001) and modified for use in this activity as described below. This effort thus begins the task of pulling apart CMC characteristics to see which has the most significant impacts on this type of relationship. This cyberstalking severity model and each of its specific constructs are described in greater detail in the following sections.

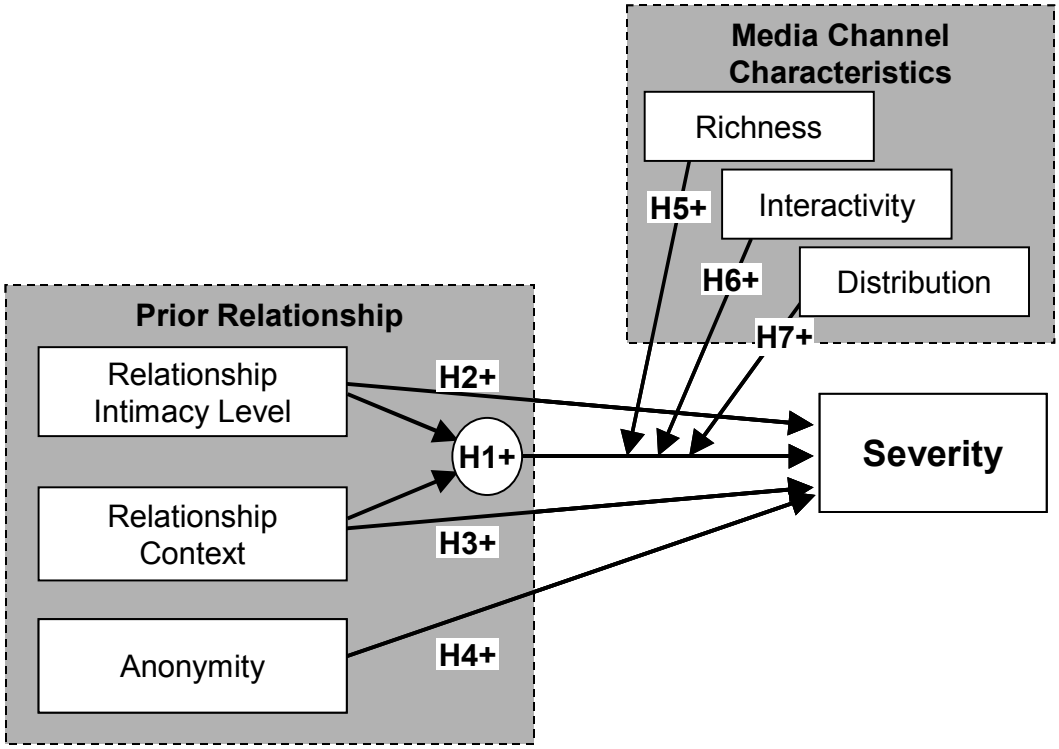


Figure 2: Cyberstalking Severity Model

Relationship Intimacy and Context

A relationship's intimacy level and the context in which it began are clearly related (Emerson et al. 1998). However, this effect changes the longer the relationship lasts, since the experience gained will eventually dominate the nature of the relationship (McKenna et al. 2002). Thus, there is the likelihood for interaction between these two constructs and this interaction should also affect the relationship after it becomes disjunctive. This is supported with the study by Thompson and Nadler (2002) that showed that adversarial negotiations were hindered by exclusive use of CMC channels, implying that the use of CMC channels will affect at least some types of disjunctive relationships. Further, because the nature of the prior relationship is known to have an effect on stalking case severity (Emerson et al. 1998; Thompson and Nadler 2002;

Cupach and Spitzberg 2004; Hian et al. 2004), an analysis must begin by looking at the interaction between the intimacy level of the relationship and the context in which the relationship began. In this case, it requires differentiating between relationships that began or exist totally online versus those that merely include online elements. This suggests that differences in case severity will be noted when online and offline cases of stalking are compared.

While arguments can be made for either an increase or a decrease in case severity resulting from use of CMC channels, it appears that on balance, a decrease is more likely. The argument for an increase is based on extending the work of Bargh, McKenna, and colleagues (Bargh 2002; Bargh et al. 2002; McKenna et al. 2002), which suggest that CMC usage accelerates the relationship cycle, along with the findings of Thompson and Nadler (2002), which suggests that CMC usage amplifies adversarial effects in a relationship. Conversely, purely online relationships tend to move offline as they strengthen (Emerson et al. 1998; McKenna et al. 2002), suggesting that the stronger the relationship, the less likely it is to remain a purely online relationship. There is definitely a one-way flow from online to offline for the strongest relationships. The reverse is likely uncommon, but possible, for friends and acquaintances, based on observation and casual conversations with friends and colleagues. Assuming that stronger relationships lead to more severe cases of stalking, online relationships that move offline will tend to bias central tendency measures of severity, lowering values for online cases and raising it for offline cases. Unless this potential confound can be measured and accounted for, it is possible it will dominate any CMC effects in the other direction.

Two simple steps can be taken to reduce (but not eliminate) this problem when working with field data. First, offline cases where the stalker is identified as a former spouse can be eliminated, as it would be extremely unusual for couples to marry without meeting offline. This eliminates many offline cases with the strongest relationships, relationships that can be assumed not to have an online corollary. Second, any measurement of case severity must include the presence of physical aggression and violence in the case. Such actions are not possible online, but should account for a portion of any reasonable measure of case severity. Thus, this study also excludes offline cases that include occurrences of physical aggression and violence from the offline comparison group.

Measurement and testing confounds aside, the following set of four hypothesis is proposed to capture the interaction between the relationship intimacy level and its online or offline context.

H1: The difference in severity levels between online and offline cases are positively related to the level of relationship intimacy.

H1A: Case severity levels associated with offline intimate relationships will be more severe than online intimate relationships.

H1B: Case severity levels associated with offline relationships with friends and acquaintances will NOT be different from online relationships with friends and acquaintances.

H1C: Case severity levels associated with offline relationships with strangers will be different than online relationships with strangers.

Bargh notes that online effects associated with social activity "depend on how the unique qualities of Internet communication modes interact with the particular characteristics and goals of the individuals, groups, and communities using them" (Bargh 2002 p1). These hypothesis assert that the same holds true for disjunctive relationships. The secondary hypotheses H1A, H1B, and H1C are based on different levels of experience in the relationship prior to the onset of the harassment. These hypotheses assume that as the level of intimacy increases, the importance of the communications process changes.

Intimates will have taken efforts to explore the personality and interests of their partner, but online intimates relationships are not likely to have experienced the quantity of time together as offline intimate relationships, leading to less severe cases for online intimate relationships. This leads directly to hypothesis H1A. Hypothesis H1A is, as noted above, also likely to be affected by the one-way flow of relationships from online to offline as intimacy increases, and case severity will thus reflect the increased familiarity that offline relationships have over online relationships.

Friendships are based on shared common interests, and acquaintances on shared common goals (Lewis 1960). Neither common interests nor common goals expand experience in the same manner as does intimacy, thus leading to lower levels of severity for cyberstalking cases originating out of friendships and acquaintances, when compared to intimate relationships. Further, there is nothing obvious suggesting that shared goals accomplished online differ from similar goals accomplished offline in their impact on relationships. If that is true, than it holds that when such relationships turn disjunctive, the resulting severity levels should be similar, leading to hypothesis H1B.

Strangers do not share anything at the onset of the relationship, and will thus have little knowledge on which to base their harassment actions. Further, there is little in the literature suggesting that stalking and harassment by strangers differs from that by stalkers known to the victim (Sheridan et al. 2001b; Spitzberg 2002; Spitzberg and Hoobler 2002). Thus, it is difficult to predict the relative levels of case severity between online and offline stalking by strangers, and this project will predict a difference as provided for in H1C, but will not specify a direction at this time.

Figure 3 illustrates the predicted outcome of a test of hypotheses H1, H1A, H1B, and H1C, where hypothesis H1 is represented by the differing slopes of the lines shown.

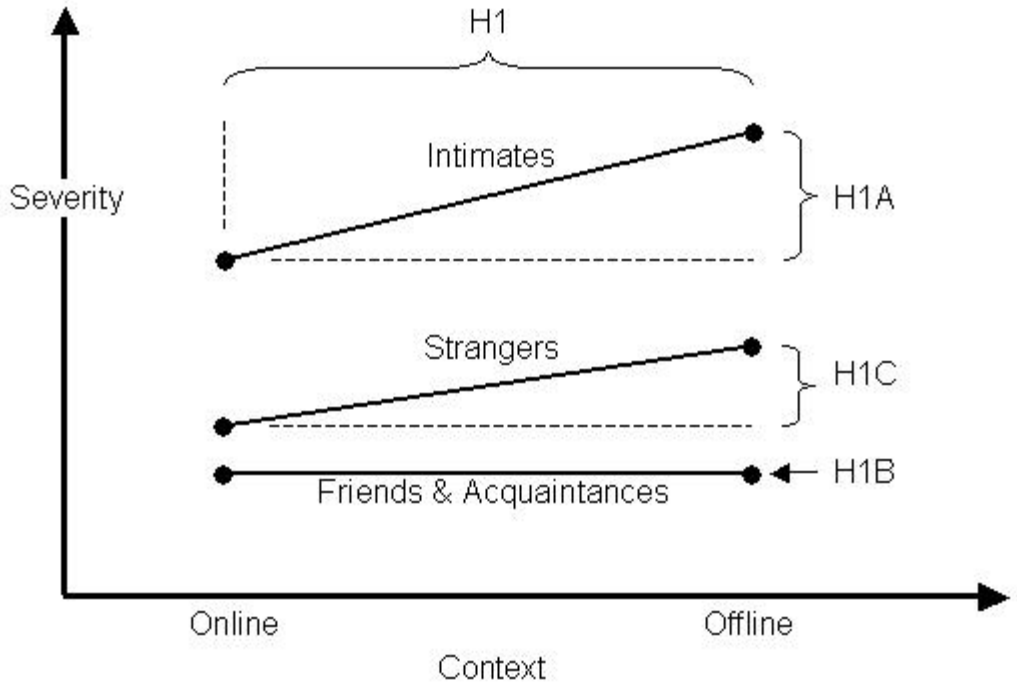


Figure 3: Predicted Results for the Relationship × Context Interaction

Main Effects: Intimacy Level

One of the more reliable findings about stalking is that the level of prior intimacy between the partners is a good predictor of violence (Cupach and Spitzberg 2004 p135,

summarizing 14 other works). Former intimates are much more likely than any others to employ aggression against their victim, with a consequent increase in the severity of the case. Purcell et al. (2004) showed that differences based on duration were correlated with the type of relationship, with longer cases associated with stronger psychological effects and greater intimacy. Taking a different perspective, the following hypothesis ignores the time domain and looks only at the reported level of intimacy and its effect on case severity.

H2: Former relationship intimacy level is positively associated with severity.

Main Effects: Context

The interaction between the intensity of a relationship and its use of CMC channels is discussed above. It is also apparent that there may be significant main effects both on relationships generally and differently on various types of relationships. These flow directly from the finding of Bargh, McKenna, and colleagues (Bargh 2002; Bargh et al. 2002; McKenna et al. 2002) and others (Kraut et al. 2002; Spears et al. 2002; Thompson and Nadler 2002; Tyler 2002) showing that Internet usage can have both positive and negative effects. Hypothesis H3 tests this generally. The direction is expected to show that offline relationships will be more severe, due to the effects of intimate relationships which are both generally more severe and more likely offline.

H3: Offline relationships will be more severe than online relationships.

Main Effects: Anonymity

Anonymity as used here is a special case within the broader spectrum of types of relationships, as noted in Chapter II. Not knowing the identity of a stalker is likely to

increase the level of fear in the victim. Further, anonymity removes the potential of negative consequences for the stalker, provided the anonymity can be maintained (Connolly et al. 1990). Given the effective ability of CMC to hide true identities (Berthold et al. 2000), a desire for anonymity on the part of a stalker is likely to influence both their choice of communications media, and the impact on the victim. Further, the more an anonymous stalker knows about a victim, the more severe the impact is likely to be. Such would be the case if a former intimate successfully stalks a victim anonymously. Thus, since CMC tools can provide effective anonymity, the impact on a case should be to increase severity. This leads to the following hypothesis:

H4: Anonymity is positively associated with case severity.

CMC Channel Characteristics

Presuming that the previous postulates hold, a logical follow-up question is what characteristic of CMC tools have the largest impact on the link between CMC usage and case severity. As shown in Table 1 and discussed in Chapter II, three characteristics of CMC media appear likely to have an impact on the outcome of a communications message (Te'eni 2001). These include the media's richness, its interactivity, and its distribution characteristics.

- **Media channel richness** addresses the capacity of the media to support more or less detail related to non-verbal cues and hints that a perceptive reader can use to interpret the message content (Te'eni 2001 p271; Kock 2004). In this research, the media used by cyberstalkers have been divided into media that

can support verbal communications, and those that only support textual messages.

- **Media channel interactivity** relates to the ability of the channel to support real time dialog between the parties (Te'eni 2001), and each media type is characterized as either real time or delayed.
- **Media channel distribution** is a proxy for Te'eni's (2001) adaptiveness, which is the ability of a medium to tailor a message for a given recipient. Media distribution is characterized as either public or private, depending on the level of control that the sender exercises over who receives the message.

This leads to three very straight-forward hypotheses about the impacts of richness, interactivity, and distribution mechanism on cyberstalking case severity, as presented below.

Media Channel Richness

Hypothesis H5 tests the impacts of the richness of media channels on communications within a disjunctive relationship, by comparing cases that use media supporting verbal communications with those that use only media supporting text. This follows from Kock (2004), who suggests that support for voice is the most important division with respect to media channel richness. To test this, each media type is characterized as either verbal or textual, and cases are categorized by their media usage information. Figure 4 illustrates the predicted impact of this richness construct on stalking case severity.

H5: Cases using verbal media will be more severe than cases using only text media.

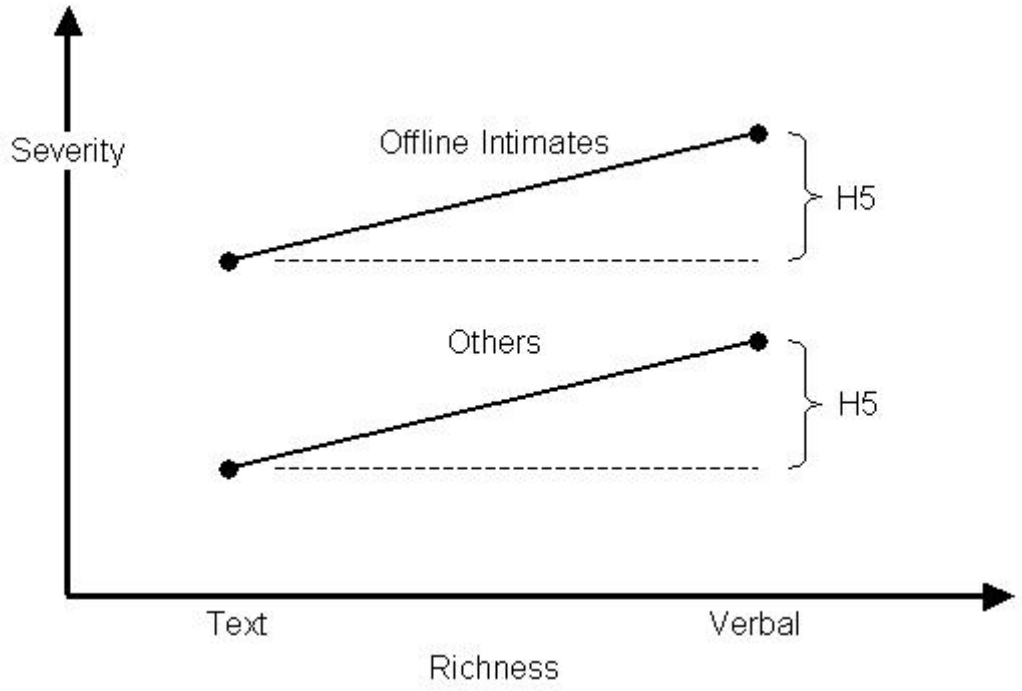


Figure 4: Predicted Impact of Richness on Case Severity

Media Channel Interactivity

As noted in Chapter II, the interactivity of a channel relates to its support for immediate feedback from the receiver (Te'eni 2001). Te'eni suggests that better interactivity assists in activities that are highly dynamic, and is necessary when the speaker must adapt the communications on the fly in response to feedback from the receiver. In disjunctive relationships, the evidence suggests that such feedback is neither required in every situation that leads to increases in case severity (Miller 1999a; Sheridan et al. 2001a) nor is it necessary for more severe acts of harassment (Spitzberg 2002). This leads to a balance of alternatives, making a specific prediction problematic. Thus, while hypothesis H6 suggests that interactivity does have an impact on case severity, it should come as no surprise if there are no differences between the types of media are found. To test this, each media type is characterized as either real time or delayed, and cases are

categorized by their medial usage information. Figure 5 illustrates the predicted impact of this interactivity construct on stalking case severity.

H6: Cases using real time media will be more severe than cases using only delayed media.

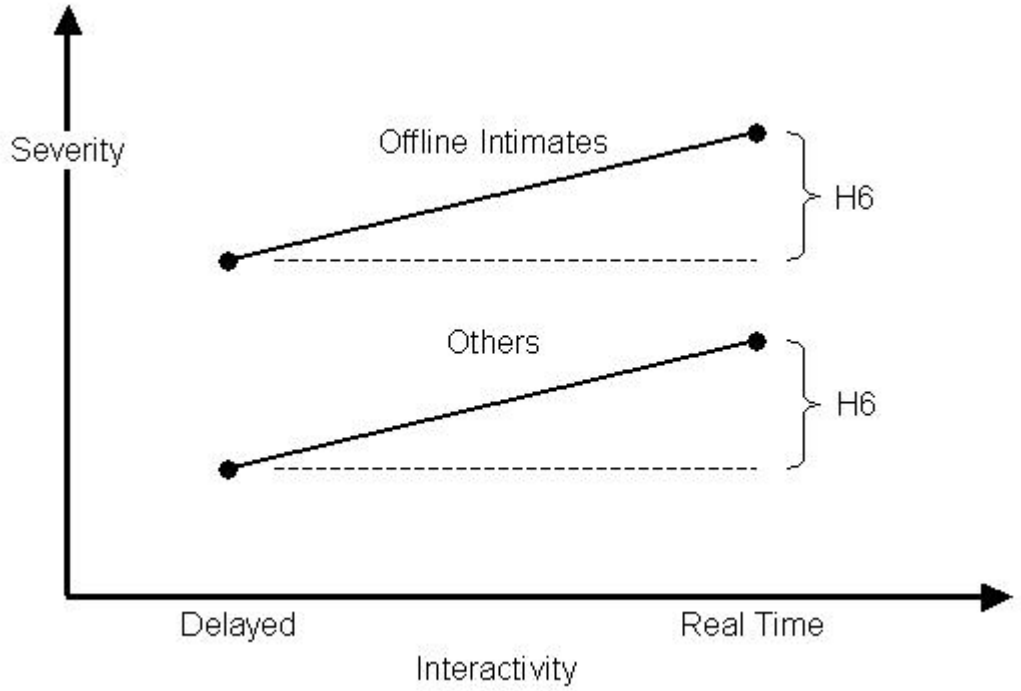


Figure 5: Predicted Impact of Interactivity on Case Severity

Media Channel Distribution

As noted in Chapter II, distribution reflects the ability of the sender to direct a message to a controlled list of recipients, and is a proxy for Te'eni's (2001) adaptability construct addressing the ability of the sender to customize or adapt a message to a particular recipient. To test this, each media type is characterized as either public or private, and cases are categorized by their media usage information. In developing a specific hypothesis for disjunctive relationships, note that some harassing activities (e.g. slander and other forms of reputational harassment) are more effective in public media,

while others are better suited to private media. As for the interactivity construct, this suggests a potential confound and leads to a balance of alternatives, making a specific prediction problematic. Hypothesis H7 tests the proposition that the distribution mechanism will affect case severity, with the stipulation that there is insufficient prior evidence to suggest that a difference between pubic and private media will be found. Figure 6 illustrates the predicted impact of this distribution construct on stalking case severity.

H7: Cases using private media will be more severe than cases using only public media.

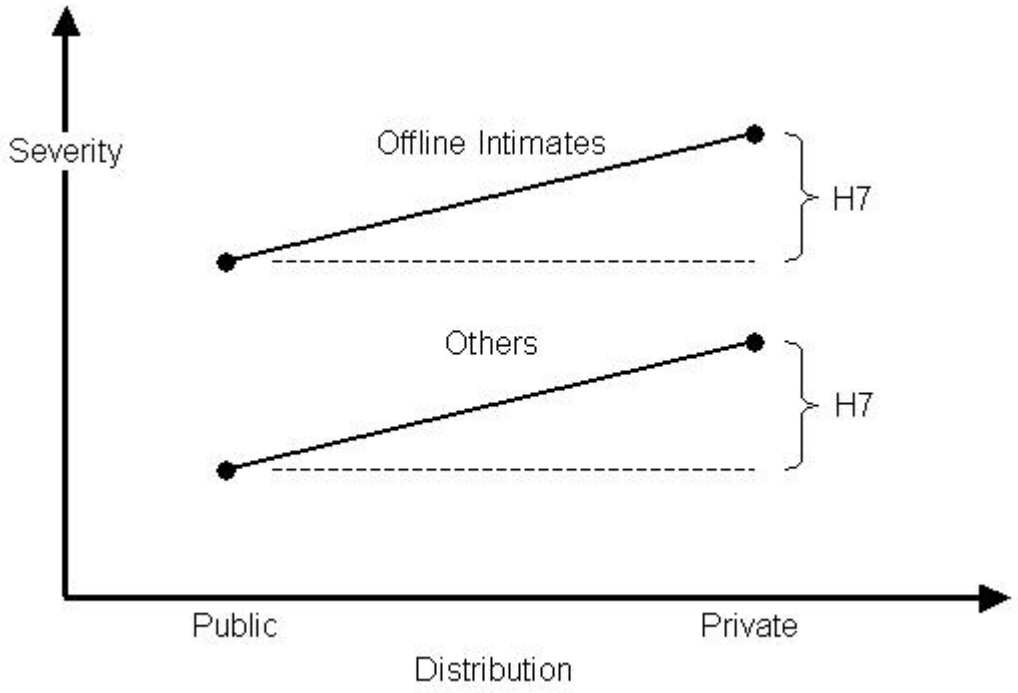


Figure 6: Predicted Impact of Distribution on Case Severity

Chapter Summary

This chapter proposes a research model to explore disjunctive stalking relationships within the confines of online computer mediated communications and offline communications. It also examines disjunctive relationships that exist only in an online context and offline relationships that use online communications tools. To accomplish this, three hypotheses are developed to test for differences in case severities and identify the most important elements of this combination of online tools and relationships. A follow up hypothesis explores whether anonymity has an impact on the severity of cyberstalking case. Finally, three possible impacts that the use of CMC media may have on the severity of cyberstalking cases are explored, and hypotheses that test for the presence of these impacts are identified.

CHAPTER IV

METHODOLOGY & ANALYTICAL APPROACH

This chapter presents information about the data used for this study and how it was transformed before the analysis. Implementation of three independent variables representing the characteristics of the media channels used is described here, as are the implementation of variables for relationship intimacy, context and anonymity of the harasser. Core to this research is the development of the dependant variable, cyberstalking case severity, which is derived from field data with the help of the Analytic Hierarchy Process (AHP) (Saaty 1994). As was noted in Chapter II, the case severity value developed here is necessarily a proxy for the true, psychological, impact of the stalking and harassment actions (Goldberg et al. 1997; Purcell et al. 2004), since the data available does not contain the relevant information. This is followed with a description of the statistical techniques used, along with a necessary correction to the dependant variable that transforms it into a normal distribution.

Data Source & Description

A victim's advocacy group, Working to Halt Online Abuse (WHOA), generously provide their cyberstalking case records for this project's use. WHOA regularly works with victims referred by law enforcement agencies otherwise unable to meet the victim's needs, and in turn refers victims to appropriate law enforcement agencies when a case is

sufficiently serious. WHOA provided 1225 case records summarizing cyberstalking incidents over the time period from 2001 to 2005. After the data was recoded (see next paragraph for the details), seventy-five cases were deemed not harassment (most were spam problems), and were dropped from the data. This left 1150 harassment cases for subsequent analysis. All data is self-reported by the victims, as recorded and summarized by WHOA's volunteer advocates (case workers). Case results are noted by the advocate, but cannot be verified. However, victims seeking help have greater incentive to provide accurate information.

Raw WHOA data was recoded into a form suitable for statistical analysis, then assigned a calculated index of apparent severity, as described below. Due to the large number of cases and items per case in this data set, one individual coded the entire data set. As a check on this process, three graduate students not otherwise associated with the project were recruited and each was asked to code a different random sample of 100 cases as a check of the coding process. Each was provided with written instructions (included as Appendix A) and a brief training session. Inter-rater reliability scores were calculated for the combination of all four coders ($\alpha = 0.947$), and for each test coder separately against the primary coder's version (α's of 0.940, 0.950, and 0.809). The primary coder's version was used for all subsequent analysis.

WHOA case data captures the communications media used for the first harassing message, other media used, other places the victim reported the harassment (e.g. law enforcement), a summary of the case results, and the year of occurrence. Each case contains some demographic information on the victim's age, gender, marital status, race, and state or country of residence. This information is summarized in Table 3. In addition,

each case contains some information about the stalker, where known to the victim, including age, gender, and state or country of residence. This project cannot address relative severity by sexual orientation, since WHOA data ignores this factor. This prohibits a direct one-to-one comparison with the study by Finn (2004).

Table 3: WHOA Data Demographic Information

	Victim		Stalker			Victim	
Age Range	**N**	**%**	**N**	**%**	**Marital Status***	**N**	**%**
Unknown	91	7.9%	849	73.8%	Unknown	115	10.0%
Under 18	5	0.4%	9	0.8%	Single	483	42.0%
18-30	549	47.7%	101	8.8%	Married	351	30.5%
31-40	311	27.0%	82	7.1%	Separated	27	2.3%
41+	194	16.9%	70	6.1%	Divorced	113	9.8%
Multiple	0	0.0%	39	3.4%	Life Partner	52	4.5%
Total	*1150*		*1150*		Widow	9	0.8%
					Total	*1150*	
Gender					**Race***		
Unknown	33	2.9%	170	14.8%	Unknown	107	9.3%
Female	857	74.5%	331	28.8%	African American	44	3.8%
Male	260	22.6%	606	52.7%	Asian	40	3.5%
Multiple	0	0.0%	43	3.7%	Caucasian	837	72.8%
Total	*1150*		*1150*		Hispanic	47	4.1%
					Native American	22	1.9%
					Other	53	4.6%
					Total	*1150*	

*WHOA does not collect marital status or race information about harassers.

Unfortunately, WHOA advocates added variance to the data. Cases are distributed to advocates based on workload and availability. WHOA reports that distribution of cases is not based on difficulty or advocate skill set, though some appear to handle mostly international cases. In practice, some advocates provided much more detail than others in their summaries, and the data summarized changed slightly over the five years[2]. Thus, for example, 557 cases did not have sufficient information in the summary to capture any of the stalker activities used for the estimate of severity, leading to activity factor scores of 0.00 (see the next section for the method used to calculate this value). Another 343 cases

[2] This affected the prior relationship data most: in 2001 this was reported as yes/no, and then evolved in 2002 to include the type, e.g. ex intimate, family member, coworker, employer, fellow student, etc.

reported only the presence of one or more unspecified threats. It is also highly likely that not all activities relevant to the severity were recorded in the remaining cases, leading to underestimation of the severity of most cases in the data. An even 100 cases had composite severity scores of 0.00, and yet were deemed harassment by WHOA's advocates. Univariate ANOVA was used to test the data for severity differences by advocate, and found two (of 20) outlier advocates representing 9 (0.8%) of the cases, one with a low mean severity score (2 cases), and one with a high mean score (7 cases). A post hoc test using Tukey's HSD method grouped the remaining 17 advocates together with a significance level of 0.101. One advocate contributed only one case, and was excluded from this analysis. Given the relatively large number of "insufficient data for activity classification" scores, the indicated differences with the outlier advocates were discounted, and the analysis proceeded.

The Independent Variables

The model presented above includes six independent variables. Three are derived from information about the computer mediated communications media used by the harasser to communicate with the victim. These include the richness of the media in terms of its ability to support voice or text communications, the interactivity of the media, or its ability to support real time bi-directional communications, and the distribution mechanism for the media, specifically if it is private peer-to-peer or a posted public media. The second three are related to the nature of the relationship between the stalker and the victim. These include the degree of intimacy between the parties, the context in which the relationship exists (online or offline), and if the harasser is acting (or

attempting to act) anonymously. The methods used to operationalize each of these six variables are described in the following paragraphs.

Media Channel Characteristics

The WHOA data identified 30 distinct ways harassers used CMC media to attack their victims. The data as coded included both the first media used by the harasser, and all media mentioned for use in this analysis. Table 4 shows the common forms of communications media used by stalkers in the WHOA data, along with the number of times they appeared in the data, both initially and overall. Also included were offline harassment techniques mentioned (most cases did not have any details) as one category, since they can be used as a proxy for face-to-face (F2F) communications generally. Table 5 lists the other, mostly indirect, harassment techniques identified in the data, each with the number of cases mentioning that media or technique. These are included in the "Other" media type in Table 4.

Table 4: Common Media Types and their Characteristic Classifications

Media Type	Initial Use	n	%	Richness	Interactivity	Distribution
Email	423	647	56.3%	Text	Delayed	Private
Phone	27	170	14.8%	Verbal	Real Time	Private
IM	151	293	25.5%	Text	Real Time	Private
Chat	106	148	12.9%	Text	Real Time	Public
Blog	16	32	2.8%	Text	Delayed	Public
List Groups	29	49	4.3%	Text	Delayed	Public
Website	87	170	14.8%	Text	Delayed	Public
Message Boards	166	220	19.1%	Text	Delayed	Public
Usenet	25	34	3.0%	Text	Delayed	Public
Offline	42	96	8.3%	Verbal	Real Time	Private
Post	4	50	4.3%	Text	Delayed	Private
Hacking	9	43	3.7%	Text	Delayed	Private
Ebay*	35	44	3.8%	Text	Delayed	Public
Game Forums	15	19	1.7%	Text	Real Time	Public
Other	15	37	3.2%			

*"Ebay" represents ratings of buyers and sellers in online auctions and other forms of person-to-person transactions generally.

Table 5: Other Online Harassment Techniques

Harassment Type	Initial Use	n	Richness*	Interactivity*	Distribution*
Delivered Gifts	0	1	Other	Other	Private
Ecards	2	4	Text	Delayed	Private
False Reports	0	1	Other	Delayed	Private
FAX	0	3	Text	Delayed	Private
Identity Research	0	1	Other	Delayed	Private
Impersonation	1	1	Other	Delayed	Other
Online Class	0	1	Verbal	Real Time	Public
Paging	1	1	Text	Delayed	Private
Photos Posted	0	2	Text	Delayed	Public
Radio	0	1	Verbal	Real Time	Public
Spyware	1	1	Text	Delayed	Private
Texting	0	8	Text	Delayed	Private
Unwanted Subscriptions	1	2	Other	Delayed	Private
Webcam	0	2	Verbal	Real Time	Private
Webring	1	1	Text	Delayed	Public
Wikipedia	0	2	Text	Delayed	Public
Unknown	8	5**			

*In these columns, "Other" characterizations were not used when classifying a case.
**There were 5 cases that did not mention any media at all, and were excluded from the media impact analysis.

To complete the analysis, all 30 harassment types found in the data were characterized in three ways to align with those suggested in Chapter II and III above: 1) by their richness, 2) by their interactivity, or 3) and by their distribution characteristics. This is shown in the last three columns of Tables 4 and 5 above. Since each case could, and often did, use multiple media, the cases were assigned to a "mixed" classification if the case combined media that differed in characterization in that category. Thus, if a case included both email and phone as coded, then the case classification would be "mixed" richness, "mixed" interactivity, and "private" distribution. Table 6 summarizes the number of cases in each classification.

Table 6: Media Classification Summary

Richness		Interactivity		Distribution	
Text	901	Delayed	584	Private	512
Verbal	20	Real Time	199	Public	266
Mixed	224	Mixed	362	Mixed	367

The analysis reported in Chapter V excludes 100 cases involving former spouses, family members, serious aggression, cases that began online then moved offline before the harassment began, and 5 cases that did not provide information on the media used by the harasser. The reasons for these exclusions are explained in the next section.

Prior Relationship Level of Intimacy and Context

The most important independent variable in this project's working model is the victim-perpetrator relationship, which is expected to control for the traditional view (Sheridan et al. 2001a) that the presence of a strong relationship increases the severity of the case. Therefore, the cases were categorized by prior relationship, using and extending the categories provided by Sheridan et al. (2001a). Prior relationships and the context where the relationship existed are clearly related. Cyberstalking implies an online component, and there are many cases of purely online stalking. To capture this element, each case was coded as purely online, originally an offline relationship, or relationship context unknown. In addition, four cases were identified in the original data as having originated online, but moved offline prior to the onset of harassment. Due to the small number of such cases, they were excluded from the analysis.

The WHOA data provides excellent information about prior relationships between the victim and stalker for the years 2002-2005. In 2001, WHOA recorded the existence of a relationship, but not its nature. The WHOA data was coded into 7 categories as shown in column 2 of Table 7. Column 1 maps the WHOA categories into the categories defined by Sheridan et al. (2001a) for prior relationships, specifically former intimate/spouse, acquaintance, stranger, unknown, plus one category suggested by Roberts and

Dziegielewski (2006), other family member. Table 7 also shows the breakdown of each category by the context of the case.

Table 7: Prior Relationship Categories

Sheridan Category	WHOA Relationship	Purely Online	Originally Offline	Context Unknown
Intimate/Spouse	Spouse	0	56	0
	Intimate**	49	95	21
Acquaintance	Friend	23	36	10
	Acquaintance	178	159	13
Other Family	Family	0	15	0
Stranger	Stranger/None	266	7	15
Unknown	Unknown	81*	8*	114*
	*Unknown in 2001:	22	5	47

*74 of these 203 were in 2001, when WHOA did not generally record the nature of the relationship. There were a total of 249 cases recorded in 2001.
**Excludes 4 cases that began online and moved offline before the harassment began.

Because the two categories "Spouse" and "Family" did not have any online or unknown relationships, they were excluded from further analysis. In addition, there were 20 cases that identified significant acts of aggression. As this can only occur offline, these cases were excluded as well. Four intimate cases were excluded because the case record showed that the relationship began online and moved offline before the harassment began. The small number of such cases does not allow a meaningful statistical analysis to be preformed on these cases. Finally, all cases where either the prior relationship or the context were coded as "unknown" were dropped, leaving 789 valid and complete cases.

Anonymity of the Harasser

Each case was coded as anonymous (n = 277), not anonymous (n = 649), or unknown (n = 179). This was not derived solely from Table 7 data on relationships, but also from other evidence in the case summary. The anonymity analysis below excludes the cases marked as anonymity unknown.

Case Severity – The Dependent Variable

Researchers studying computer mediated communications generally measure the outcomes of their tasks using measures of either performance (Carlson and Zmud 1999) or perception (Daft and Lengel 1986), and tend to overlook alternative measures of task success, such as the emotional impact it can have on the recipient (Te'eni 2001). The true impact of stalking is the impact it has on the victim (Goldberg et al. 1997; Purcell et al. 2004), which meets Te'eni's requirements for the output of a communicative act (Te'eni 2001). As noted above, there are few measures of incident severity related to stalking or cyberstalking in the literature. According to classic stalking research (Emerson et al. 1998; Cupach and Spitzberg 2004; Purcell et al. 2004), an increase in the number and severity of stalking events translates into an increasing impact on the victim. Supporting this, Purcell et al. (2004) showed a connection between the frequency and number of harassing acts, threats, and aggression and the resulting psychological impact on the victim. This suggests that measures of duration, action frequency, threat volume, and aggression can act as proxies for measures of the psychological impacts of stalking on victims. Such an index of case severity is developed in this section, based on the categories of stalking activities and strategies developed by Spitzberg (2002) augmented with additional categories suggested by Sheridan et al. (2001b) and a preliminary review of the data recorded in the case summaries provided by WHOA. The resulting index of case severity corresponds to CAMOC's communications message impact (Te'eni 2001), and is used as the dependent variable for this study.

To develop the index of case severity, the WHOA case data was used to calculate three category scores, based on the actions taken by the stalker, any threats present in the

case summary, and on the results noted by the WHOA advocate. These category scores are weighted and summed to provide the overall case score. To implement the approach, each case is scored with a Boolean value showing the presence (or not) of each specific type of activity, threat, or result, respectively, within each category as described below. The index of case severity is then calculated as the sum of the products of the item weights times the item's presence flag. Analytic Hierarchy Process (AHP) was used to provide weights for each item within each category and for the category weights (Saaty and Vargas 2001; Taylor 2004). The details of each category and the specific actions included in each are described in the following subsections, along with details on the use of AHP in the calculation of the item weights. More information on AHP and how the weights were calculated is included in Appendix B.

Harassing Activities

Spitzberg's (2002) stalking typology, which lists a large number of harassing activities that have been identified by earlier researchers as symptoms of stalking, provides the basis for the activity component of the case severity index. This meta-analysis groups the activities into seven broader categories with roughly increasing levels of severity. Spitzberg's list include some of the less severe harassment activities that fit into the non-stalking categories identified by Sheridan and colleagues (Sheridan et al. 2001b; Sheridan et al. 2002) in the intimidation and harassment category. Deferring to Sheridan and colleagues, since their analysis is based on a cluster analysis of responses to a targeted survey, such activities are included in a less severe "obnoxious" or "obscene actions" category. For completeness, Sheridan's "non-stalking courtship" category was also added to Spitzberg's list along with a category for cases with insufficient

information for categorization. This provides a full range of traditional harassing and stalking behaviors, which is presented in Table 8, along with AHP-based weights which are explained below and in Appendix B.

Table 8: Stalking and Harassment Activity Categories

Activity Category	Spitzberg Category*	N	AHP Weight
Aggression	VII	23	0.316
Coercion and Constraint	VI	1	0.273
Intimidation, Slander, & False Charges	V	231	0.085
Hyper Intimacy	I	52	0.078
Impersonation		69	0.060
Invasion, Theft, and Vandalism (excluding hacking)	III	87	0.049
Proxy Pursuit & Intrusion	IV	45	0.045
Pursuit, Proximity, Surveillance	II	69	0.036
Obnoxious or Obscene Actions		551	0.023
Courtship behavior		35	0.022
Hacking, Trojans, Spyware, and Targeted Viruses		60	0.013
Insufficient data for activity classification		557	0.000

*See Table 2 for full definitions of Spitzberg's categories.

The WHOA data, being field data related to online harassment, included cases that did not easily fit into any category identified by Spitzberg or Sheridan and colleagues (Sheridan et al. 2001b; Sheridan et al. 2002; Spitzberg 2002) and that were specifically online in nature. These included impersonation of the victim by the stalker, and the uses of information technology to vandalize or otherwise harass the victim, or "hacking". For example, a computer virus can be used to simply damage a victim's computer, or can be used to place Trojan horse software, allowing access to passwords or track online activity. Information thus gleaned by the harasser can be used for theft of information, access to online accounts, and impersonation, intimidation or slander. Since it is not obvious where these online activities belong within the categories from earlier research, two additional categories are included in Table 8 to capture cases that mentioned these activities.

Each case is scored with a 1 to identify the presence of one or more activities in a category, or as a 0 in each category if there were no activities in that category in that case. Thus, cases can show activity in multiple categories, but do not show the relative level of activity within a category, since this is not captured or recorded by WHOA. These are used to generate the activity factor for the case. To generate the activity factor score, the coded value for each category is multiplied by the AHP weight for that category, and summed to give a factor score between 0 and 1.

Threats

WHOA specifically asks victims about threats, and their case summary data includes a large number of cases where threats are present. This is used to develop a second severity factor, the threat factor. Spitzberg's Intimidation and Harassment category includes a variety of threat types that were found in 419 of the 1150 (36.4%) harassment cases. To better analyze this data, the threat information is separated into five threat categories, shown in Table 9, based on the types of threats mentioned in Spitzberg's meta-analysis (2002) and included in his intimidation and harassment category.

Similar to the activity factor, the presence of a threat in the case was recorded as a 1 in the category and as 0 otherwise. To generate the threat factor score, the coded value for each category is multiplied by the AHP weight, and summed to give a factor score between 0 and 1.

Table 9: Threat Categories

Threat Category	N	AHP Weight
Death threats & threats of injury to victim	66	0.411
Threats to friends, family, or pets	8	0.358
Other threats and all unspecified threats	343	0.136
Threats to release personal information	44	0.054
Threats to property	10	0.042

Case Results

In the case summaries, WHOA advocates capture a brief statement of the results of their part of the case. In many cases, this is not the totality of the activity on the part of the greater team supporting the victim. A majority of cases, however, had sufficient information to develop a severity factor based on these comments. Note that this can be considered a lower bound on the resulting impact, as WHOA may not have known about or recorded more severe events in any given case. The result data was classified into one of 33 main result types. Because 33 types are too many to achieve reasonable results with the AHP process, similar result codes were combined, ending with 13 result categories, with the corresponding AHP weight used as the result factor score for the case, as listed in Table 10. Note that the last two categories in Table 10 are null categories with respect to their impact on the factor score.

Table 10: Result Categories

Result Category	N	AHP Weight
Criminal charges pending	24	0.338
Restraining order requested or issued	43	0.219
Referred to law enforcement agency, under continuing investigation	160	0.144
Referred to an attorney	36	0.094
Harasser banned by service provider (SP) or blocked by victim	74	0.057
Reported to SP for action under terms of service	163	0.042
Other (diverse) results	3	0.042
Changed online identity	245	0.024
Victim stopped using service	98	0.017
Offending material or website removed	19	0.013
Ended or victim ignoring harassment	56	0.010
Victim ignored WHOA advice or is harassing harasser	46	0.000
Unresolved or unknown as victim failed to respond to follow-up process	183	0.000

AHP Severity Factor Weights

The Analytic Hierarchy Process was developed by Saaty and Vargas (Saaty 1994; Saaty and Vargas 2001) and presented in a form suitable for calculation using spreadsheets by Taylor (2004). AHP uses pair-wise comparisons of alternatives by a subject matter expert to develop a preference (severity) vector for each criterion factor and factor category item (Saaty and Vargas 2001). The output can be thought of as the distance between the items on a linear scale, with an overall range of 0 to 1. In this case, Taylor's (2004 p372) method was used to get weights for three main factors: activities, threats, and results that have been coded from the data. More detail on how this process was implemented can be found in Appendix B. These weights are presented in Table 11. Then for each main factor, the process was repeated on the component fields for that factor, resulting in the AHP weights given in Tables 8-10.

Table 11: Factor Weights

Severity Factor	AHP Weight
Activities	0.623
Threats	0.239
Results	0.137

The weights in Table 8 and Table 9 were derived using inputs provided by surveying a small number of professionals currently working in the domestic violence field, and asking them to estimate the difference in severity between pairs of activities, and pairs of threats. The trio of respondents included an investigative detective from a large metropolitan police force specializing in stalking and domestic abuse cases, and two members of a coordinating council on domestic violence serving the same metropolitan area. The questionnaire used for this process is provided in Appendix C. Inter-rater reliability for the three respondents was $\alpha = 0.820$. The results of this survey were averaged item by item per Saaty (1994) and input into AHP to develop the category weights given above. Note that our trio of experts did not agree with the activity severity ordering suggested by Spitzberg (2002) and shown in Table 8. The result weights derived in Table 10 and the factor weights in Table 11 used AHP inputs generated by this researcher in consultation with WHOA.

Statistical Methods

ANOVA is the statistical analysis method of choice when the independent variables are categorical and the dependant variable is scalar (Pedhazur and Schmelkin 1991; Hair et al. 1998; Freund and Wilson 2003). While regression provides the same results, it is more difficult to code categorical data for regression, due to the requirement that categorical data be dummy coded. Additionally, ANOVA cleanly and clearly isolates

interaction terms and results in factorial designs where the results sought are likely to show the existence of complex interactions. Thus the bulk of the analysis in this project utilized ANOVA methods.

Use of ANOVA requires that the error variance of the dependent variable is equal across groups (Hair et al. 1998; Freund and Wilson 2003). Since the nature of cyberstalking case severity is such that mathematically it appears exponential, our data violates this assumption. The solution to this problem is straight-forward: transform the dependant variable in such a manner that it approaches a normal distribution. The AHP process results in a severity index value that is between zero and one, with the bulk of the values at the lower end of this range. Only 17 cases in this data set of 1150 cases have a severity index greater than 0.4. The most appropriate transformation for this data set is to take the cube root of the index value, which was found to minimize the skewness for the transformed data. The impact of this transformation on the WHOA cyberstalking data is captured in Table 12 below. The transformed value was used in all testing of this data. Since the AHP severity index is a calculated index, using a transformation does not present any interpretation problems with respect to understanding the data under analysis in this situation (Hair et al. 1998).

Table 12: Dependant Variable Transformation

	Untransformed	Transformed
Mean	0.0495	0.2960
Standard Deviation	0.0640	0.1617
Kurtosis	9.5997	-0.4132
Skewness	2.5482	0.0730

ANOVA has been used to study similar, non-random field data in a variety of disciplines. Roth and Morrison (1990) used ANOVA to analyze data from selected large enterprises to study the integration-responsiveness framework in global industries.

Lubatkin et al. (1997) used non-random samples to study the Universalist hypothesis of management work using data from managers in four countries selected for organization size and culture. Snodgrass et al. (2006) used MANOVA to analyze non-random, cross-sectional data documenting the prevalence of obesity among indigenous populations.

CHAPTER V

RESULTS

Following the logic presented above, this report must first present the results of the interaction between the relationship intimacy level and the context in which the relationship began and exists. Once these constructs are characterized, the analysis proceeds to the impacts of CMC media on the case severity, which is the focal point of this research project. The chapter concludes with a post hoc analysis of the impacts of specific media types (e.g. email) on case severity, and the relationship between gender and case severity.

Relationship Context and its Effect on Cyberstalking Severity

Relationship Intimacy by Context Results (H1)

Hypothesis H1 postulated an interaction between the relationship intimacy level and relationship context variables. The analysis used a 2 x 3 factorial design in an ANOVA framework to test for this interaction. The results showed a significant interaction term, as seen in Table 13, providing support for hypothesis H1. The six interaction cell means were compared using Bonferroni's correction for multiple comparisons, and only the offline intimate cell was consistently different from the other cells. This is shown in Table 14, and the cell mean values are illustrated in Figure 7. Both

suggest that online cases are similar in severity to offline cases, except when the relationship is intimate.

Table 13: Prior Relationship by Context Interaction Results

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Observed Power(a)
Intercept	15.800	1	15.800	722.093	0.000	1.000
Intimacy	0.197	2	0.098	4.493	0.011	0.768
Context	0.361	1	0.361	16.481	0.000	0.982
Intimacy * Context	0.144	2	0.072	3.279	0.038	0.623
Error	17.132	783	0.022			

(a) Computed using alpha = 0.05. (b) R Squared = .061 (Adjusted R Squared = .055).

Table 14: Planned Comparisons of Relationship by Context Cell Means

Difference of Means *Significance*	Offline Intimates	Offline Acquaint.	Offline Strangers	Online Intimates	Online Acquaint.	Online Strangers
Offline Intimates		**0.069**	-0.055	**0.091**	**0.104**	**0.117**
		0.006	*1.000*	*0.010*	*0.000*	*0.000*
Offline Acquaint.	**-0.069**		-0.123	0.022	0.035	**0.049**
	0.006		*0.993*	*1.000*	*0.299*	*0.010*
Offline Strangers	0.055	0.123		0.145	0.159	0.172
	1.000	*0.993*		*0.550*	*0.271*	*0.153*
Online Intimates	**-0.091**	-0.022	-0.145		0.013	0.027
	0.010	*1.000*	*0.550*		*1.000*	*1.000*
Online Acquaint.	**-0.104**	-0.035	-0.159	-0.013		0.013
	0.000	*0.299*	*0.271*	*1.000*		*1.000*
Online Strangers	**-0.117**	**-0.049**	-0.172	-0.027	-0.013	
	0.000	*0.010*	*0.153*	*1.000*	*1.000*	

Bold cells are significant at the 0.05 level. Adjustment for multiple comparisons: Bonferroni.

Hypothesis H1A postulated that offline intimate cases would be more severe than online intimate cases. This hypothesis is supported ($p = 0.010$), as shown in Table 14. In the intimate case, offline cases are more severe, likely due to the closer nature of the relationship and the feasibility of offline harassment activities.

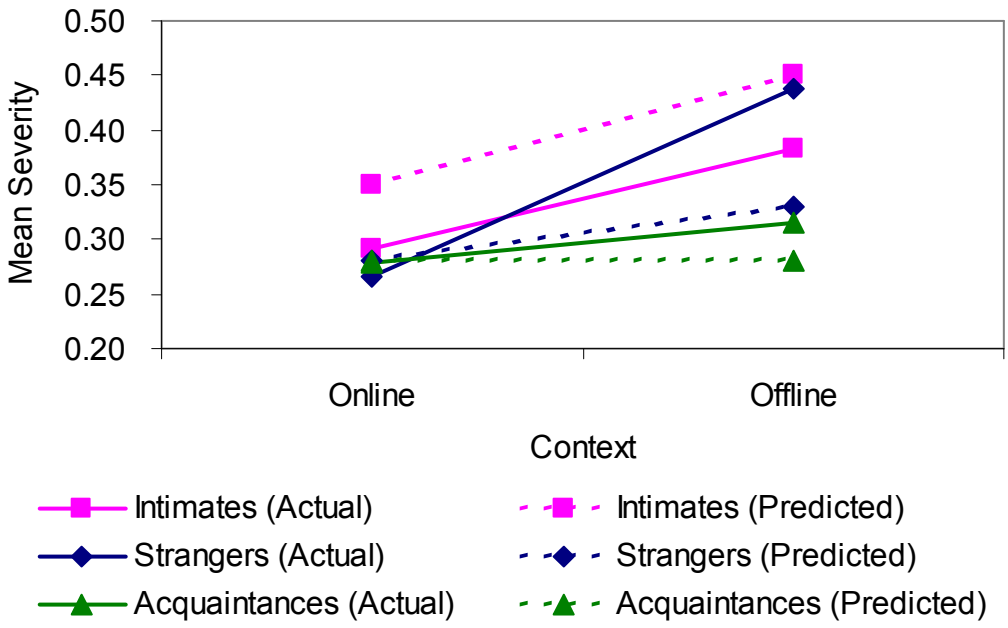


Figure 7: Prior Relationship by Context Interaction Results

Hypothesis H1B postulated that offline acquaintance cases would not be different from online acquaintance cases. This hypothesis is supported with this data ($p = 0.299$). Note that this test has excellent balance (offline n = 182, online n = 200) and a sufficient number of cases to provide a robust result. It is then possible to conclude that online only relationships at the acquaintance level are no different from their offline equivalent when disjunctive.

Hypothesis H1C postulated that offline stranger cases would be different from online stranger cases. This hypothesis is not supported with this data ($p = 0.153$). Note that while the difference between the offline and online stranger means is the largest difference shown, this is not significant due to the very small number of cases in the offline stranger category (n = 5). With additional data, it is possible that this hypothesis could be supported, thus this result is insufficient for use in drawing any meaningful conclusions.

Relationship Intimacy and Context Main Effects (H2 & H3)

Hypothesis H2 postulated a difference in case severity based on the level of intimacy in the relationship. Accounting for relationship intimacy and relationship context interaction, the intimacy main effect term was significant ($F_{(2, 783)} = 4.493$, $p = 0.011$, power at $\alpha = 0.05$ is 0.768), as seen in Table 13. Thus the data supports hypothesis H2, and indicates that intimacy level is a factor within cyberstalking cases. This follow expectations as suggested by Spitzberg's (2002) review of the stalking literature, and suggests that cyberstalking is not different from offline stalking it this area. Figure 8 charts the mean severity levels actually measured, along with the relative levels predicted above.

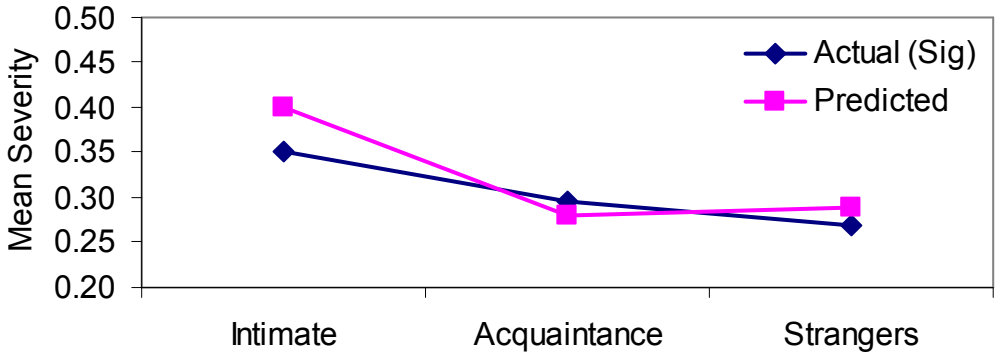


Figure 8: Independent Effect of Prior Relationship

Hypothesis H3 postulated that severity of offline cases would be more severe than those that were online. Accounting for relationship intimacy and relationship context interaction, the context main effect term is significant ($F_{(1, 783)} = 16.481$, $p < 0.001$, power at $\alpha = 0.05$ is 0.982), as seen in Table 13. This suggests that the online versus offline context of the relationship influences the severity of the case, and supports hypothesis H3. From this information we can tentatively conclude that while online disjunctive relationships are in most respects similar to those offline, an online context mitigates the

severity of a case, even after eliminating cases including offline aggression from the comparison. Figure 9 charts the mean severity levels actually measured, along with the relative levels predicted above.

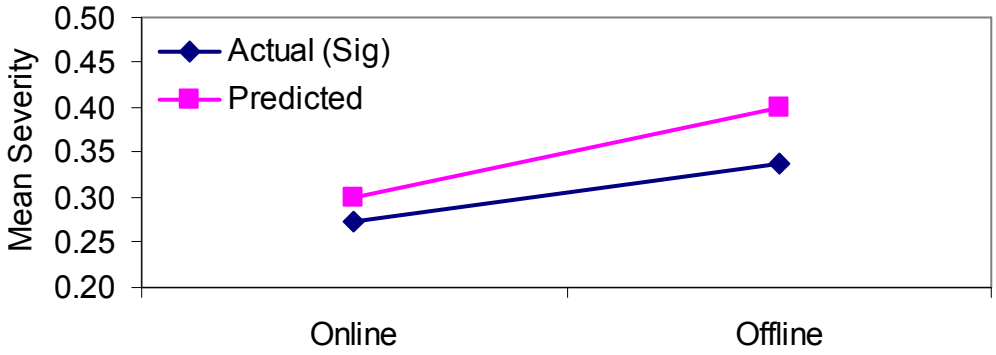


Figure 9: Independent Effect of Context

Given the concurrence of these analyses, it should be clear that context plays a significant role in the effects so far studied. Thus it is easy to conclude that the use of CMC tools dampens the effects of a harasser's efforts, leading to lower levels of case severity.

Anonymity Results (H4)

Hypothesis H4 addressed anonymity as a factor in case severity. To test this, a 2 x 6 factorial design ANOVA was employed to contrast the anonymity variable described in Chapter IV with the cells of the combined relationship intimacy-context interaction described above. This test failed to show any significant interactions ($F_{(4, 684)} = 0.801$, $p = 0.525$, power at $\alpha = 0.05$ is 0.258). Anonymity as a main effect was not significant after accounting for relationship intimacy and context ($F_{(1, 684)} = 0.806$, $p = 0.369$, power at $\alpha = 0.05$ is 0.146), and a univariate test of anonymity was also not significant ($F_{(1, 684)} = 1.40$,

p = 0.237, power at α = 0.05 is 0.219). Figure 10 charts the mean severity levels actually measured, along with the relative levels predicted above.

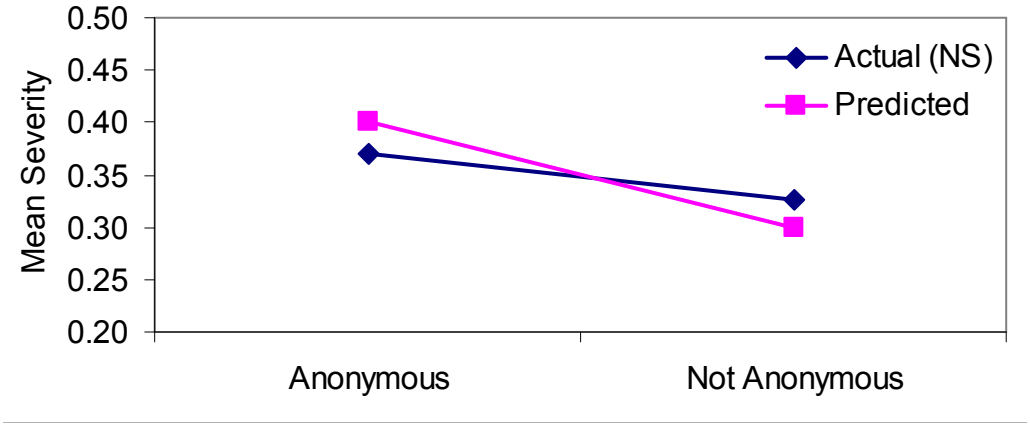


Figure 10: Independent Effect of Anonymity

Thus the data from WHOA fails to support hypothesis H4, which suggested that anonymity has a role in cyberstalking case severity. From this it is clear that this data does not support the suggestion that anonymity affects case severity in any meaningful manner.

Impacts of CMC Channel Characteristics on Cyberstalking Severity

Turning to the focal point of this research activity, the impacts of CMC channel characteristics are analyzed next. In line with the research model outlined in Chapter III, channel richness is analyzed first, followed by channel interactivity, and then channel distribution.

CMC Channel Richness (H5)

Hypothesis H5 posited that severity of cases using media supporting verbal communications would be more severe than cases using only media that support text

communications. Before looking at the main effects, the richness variable was tested against the combined prior relationship plus context variable established above to determine if the established effect of intimacy plus context affected the richness results. This interaction test failed to show a significant interaction term ($F_{(8, 773)} = 0.822$, $p = 0.583$, power at $\alpha = 0.05$ is 0.388), thus the analysis of the richness main effects term resumed. It showed that the richness construct provides a significant impact on case severity ($F_{(2, 773)} = 6.525$, $p = 0.002$, power at $\alpha = 0.05$ is 0.908), supporting the hypothesized effect. Figure 11 charts the mean severity levels actually measured, along with the relative levels predicted above.

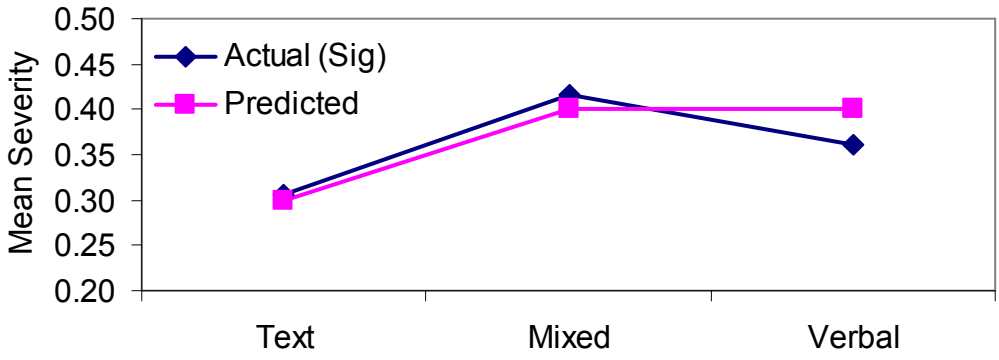


Figure 11: Chart of Media Richness Mean Severity Levels

Following up on this, the separate richness categories of verbal, text and mixed use cases are examined. Tukey's HSD test was used to associate groups that were not dissimilar. This found that text only cases are separate from the other two, as shown in Table 15 below.

Table 15: Richness Severity Means Comparison

Tukey HSD		Subset	
Richness	**N**	**1**	**2**
Text	644	0.275	
Verbal	10		0.386
Mixed	135		0.388
HSD Significance		1.000	0.998

Based on Type III Sum of Squares. The error term is Mean Square (Error) = 0.021. Uses Harmonic Mean Sample Size = 27.533. The harmonic mean of the group sizes is used. Alpha = 0.05.

Tests of the severity between classes within the richness variable showed a significant difference between text cases and mixed cases (mean difference 0.113, $p < 0.001$, using Bonferroni's correction for multiple comparisons), as did the test for a difference between text and verbal cases (mean difference 0.111, $p = 0.047$). The comparison between verbal and mixed cases failed to show a significant difference of means (mean difference 0.002, $p < 0.999$). The mean severities were ordered, with text less than verbal, and verbal less than mixed. All the tests used for this analysis concurred in this comparison, providing support for hypothesis H5, suggesting that cyberstalking case severity increases if the stalker uses media capable of supporting verbal communications.

CMC Channel Interactivity (H6)

Hypothesis H6 postulated that severity of cases using interactive media supporting real time communications would be more severe than cases using media that only support delayed communications. Before looking at the main effects, the interactivity variable was tested against the combined prior relationship plus context variable established above to determine if the established effect of intimacy plus context affected the interactivity results. This interaction test failed to show a significant

interaction term ($F_{(10, 771)} = 0.493$, $p = 0.895$, power at $\alpha = 0.05$ is 0.261), thus the analysis of the interactivity main effects term resumed. This showed that the interactivity construct provides a barely statistically significant impact on case severity ($F_{(2, 771)} = 3.183$, $p = 0.042$, power at $\alpha = 0.05$ is 0.609). Figure 12 charts the mean severity levels actually measured, along with the relative levels predicted above.

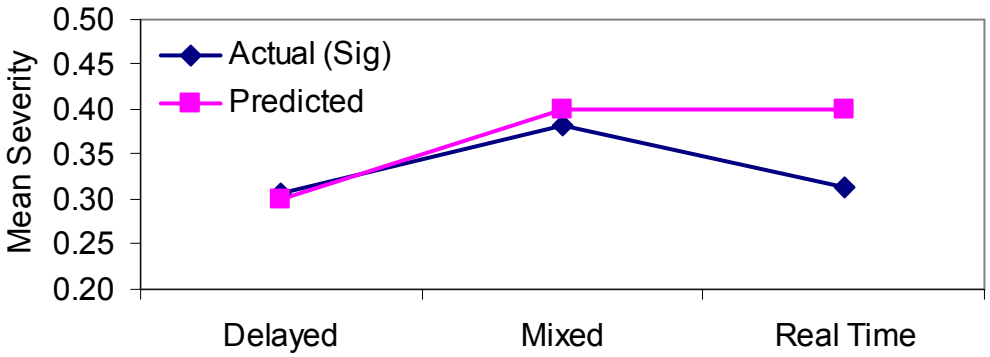


Figure 12: Chart of Media Interactivity Mean Severity Levels

The interactivity variable divides into two groups based on Tukey's HSD test: real time only and delayed only cases were not different from each other, and both were less severe than cases that used both types of media, as shown in Table 16. Tests of the severity between classes within the interactivity variable showed a (just) significant difference between delayed cases and mixed (mean difference 0.075, $p = 0.041$, using Bonferroni's correction for multiple comparisons). The test for a difference between real time and mixed cases (mean difference 0.070, $p = 0.201$), and the comparison between delayed and real time cases (mean difference 0.006, $p > 0.999$) failed to show a significant difference of means. All executed tests concurred in this comparison.

Table 16: Interactivity Severity Means Comparison

Tukey HSD		Subset	
Interactivity	**N**	**1**	**2**
Real Time	136	0.266	
Delayed	411	0.274	
Mixed	242		0.351
HSD Significance		0.834	1.000

This result is not the result that was postulated in H6. From this evidence, cyberstalking activities taken as a whole do not require particularly high levels of interactivity. This concurs with the evidence from Miller (1999a), Sheridan et al. (2001a) and others (Cupach and Spitzberg 1994; Finkelhor et al. 2000; Spitzberg 2002; Cupach and Spitzberg 2004) that immediate feedback is not required to elevate case severity associated with disjunctive relationships, and suggests that cyberstalking tasks are not associated with high levels of dynamic complexity. This evidence does not invalidate interactivity as a CMC construct, but shows that it is sensitive to the dynamic complexity of the communications task.

CMC Channel Distribution (H7)

Hypothesis H7 postulated that the severity of cases using media supporting private communications would be more severe than cases using only media that support public communications. Before looking at the main effects, the distribution variable was tested against the combined prior relationship plus context variable established above to determine if the established effect of intimacy plus context affected the interactivity results. This interaction test failed to show a significant interaction term ($F_{(9, 772)} = 1.517$, $p = 0.137$, power at $\alpha = 0.05$ is 0.725) , thus the analysis of the distribution main effects term resumed. This showed that the distribution construct fails to provide a statistically

significant impact on case severity ($F_{(2, 772)} = 0.492$, $p = 0.611$, power at $\alpha = 0.05$ is 0.131). Figure 13 charts the mean severity levels actually measured, along with the relative levels predicted above.

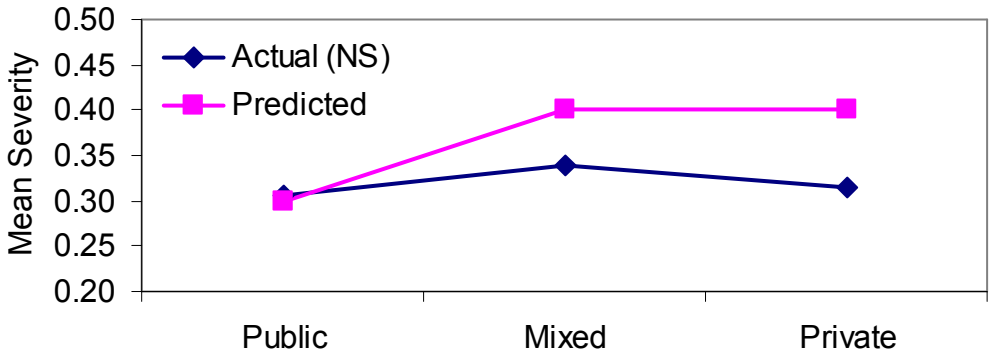


Figure 13: Chart of Media Distribution Mean Severity Levels

All executed tests concurred in this comparison. Again, this result is not the result that was postulated in H7. This result shows that control over the distribution of communications does not lead to higher cyberstalking case severity. This demonstrates that cyberstalking activities generally are not affected by the choice of distribution. However, this data and analysis fails to test for the difference in effectiveness of specific types of activities as affected by the distribution mechanism used, which is still likely to have an impact on the communications outcome.

Post Hoc Analysis

In addition to the analysis of the postulated hypothesis, the available data made it possible to examine two more questions as a post hoc activity. The first is an extension of the CMC analysis, which looks at the actual media selected by the harasser, to see if there are any interesting correlations of case severity with specific media that is not captured in

the primary analysis. The second looks at the impacts of gender, both for the victim and for the harasser, on the severity of the case. The results of each of these analysis follow.

Online Media Usage Results

Because cases often escalated using different media, leading to use of several media in a single case, the media reported for the initial harassment was used to look at case severity by media. The ANOVA results indicated significant between class differences ($F_{(14, 753)} = 3.612$, $p < 0.001$, power at $\alpha = 0.05$ is greater than 0.999). Tukey's HSD test identified two groups that strongly overlapped, as shown in the following Table 17.

Table 17: Initial Media Severity Means Comparison

Tukey HSD		Subset	
Initial Media	**N**	**1**	**2**
Unknown	2	0.141	
EBay	34	0.221	0.221
Lists	23	0.230	0.230
Instant Messaging	102	0.270	0.270
Message Boards	111	0.272	0.272
Game Forums	14	0.293	0.293
Email	278	0.294	0.294
Chat	72	0.296	0.296
Usenet	18	0.317	0.317
Blog	13	0.326	0.326
Website	60	0.344	0.344
Phone	12	0.344	0.344
Hacking	2	0.364	0.364
Offline	3		0.409
HSD Significance	24		0.426

Uses Harmonic Mean Sample Size = 8.389. Type I error levels are not guaranteed. Alpha = 0.05.

However, post hoc pair-wise comparisons failed to show any real differences between the media types. The comparisons of means failed to show significance for all combinations except for offline with Ebay, email, instant messaging, list groups, message

boards (all significant at $p < 0.005$) and chat ($p = 0.022$) (all adjusted for multiple comparisons with Bonferroni's technique). Based on this and the mean values shown in Table 17, it is evident that media that supporting voice and hacking are associated with the most severe cases of stalking, while all other types of media fail to have a significant impact on case severity. This result supports hypothesis H5, which suggested that severity will differ depending on the richness of the media used in a case, and more specifically, the ability of the media to support voice interactions. Finally, note that this result suggests support for Kock's (2004) evolution of media richness theory, the psychobiological model of communications, which suggests that conveyance of speech is the primary difference between rich and lean media.

Gender in Cyberstalking Data

A review of the literature reporting the gender of victims of cyberstalking found a discrepancy between cyberstalking and traditional stalking. In a study of the online victimization of youth, Finkelhor et al. (2000) reported that 51% of young victims of online harassment were male. Alexy et al. (2005), in studying cyberstalking among college students, reported that 42% of victims of cyberstalking were male, which is much larger than the ratio of 2.5 found by Spitzberg (2002) in a meta-analysis of 107 studies of traditional stalking. Other studies echoing Spitzberg's findings include Tjaden and Thoennes (1998), Fremouw et al. (1997) and Sheridan et al. (2002) when studying traditional stalking. While some of these authors have noted the difference, none have suggested a cause. The WHOA data used for this project includes 854 female victims (74.5%), 261 male victims (22.5%) and 34 undisclosed gender victims (2.9%), for a female to male ratio of 3.31. Excluding clearly offline cases, there are 572 female victims

(73.8%), 180 male victims (23.2%), and 23 undisclosed gender victims (2.9%), for a female to male ratio of 3.17.[3]

Gender Results

In addition to reporting gender information for use by others, the effects of both victim and harasser gender on the severity of cyberstalking cases were analyzed. The data was tested for differences in cyberstalking severity by gender. This analysis failed to find a significant interaction between victim gender and stalker gender in a 3 x 4 factorial ($F_{(5, 757)} = 1.022$, $p = 0.403$, power at $\alpha = 0.05$ is 0.368). Further, the analysis failed to find a significant interaction between the context of the relationship and either victim gender ($F_{(9, 722)} = 0.313$, $p = 0.971$, power at $\alpha = 0.05$ is 0.162) or stalker gender ($F_{(12, 722)} = 0.779$, $p = 0.673$, power at $\alpha = 0.05$ is 0.465). Thus it does not appear that particular gender combinations within a relationship play a role in the eventual severity of any particular stalking case, once a pair of parties has connected, online or off.

Separate ANOVA tests were run on victim gender and stalker gender for differences in severity by class. The test for victims failed to show any differences by class ($F_{(2, 757)} = 0.319$, $p = 0.727$, power at $\alpha = 0.05$ is 0.101), suggesting that there are no differences in severity between male and female victims. The test for stalker gender also failed to show significant differences in severity between gender classes ($F_{(3, 757)} = 1.226$, $p = 0.299$, power at $\alpha = 0.05$ is 0.330). It is then easy to conclude that the severity of a cyberstalking case is not correlated with the gender of either the victim or the stalker.

[3] Note that this lowering of the ratio supports a proposition that online harassment is less gender biased than offline harassment, but that it does not support ratios near 1.0 found by Finkelhor et al. (2000) and Alexy et al. (2005). Additionally, since this data comes from field complaints, there is a strong probability of self selection bias in this data that may be influenced by gender.

Other Results

Further exploration of the data found no differences in severity related to victim martial status, victim race, WHOA advocate, or the year the case was recorded by WHOA. Two other demographics that have been noted by other researchers to be associated with stalking, economic status (Sheridan et al. 2001a) and sexual orientation (Finn 2004), are not available in this data set, and is thus not testable.

CHAPTER VI

DISCUSSION AND CONCLUSIONS

Summary Of Findings

This research activity has attempted to identify how the use of computer mediated communications tools affect relationships that are disjunctive. To this end, a data set of cyberstalking cases from the online victim support group Working to Halt Online Abuse (WHOA) was used to test for various impacts of CMC media on the severity of the cases. The tests performed can be divided into two groups, those that address the CMC impacts on relationships between the victim and the harasser, and those that test for the impacts of CMC media on these relationships. Table 18 presents a summary of the ten hypothesis tested with this data.

These results provide some evidence that disjunctive, formerly intimate relationships are affected by the context in which they exist, particularly when that context is online. Such online cases are less severe than their offline counterparts. The positive showing of the context versus the intimacy level was expected, since other research has shown that more intimate relationships generally have more severe cases of stalking in the traditional offline context (Brewster 2000; Spitzberg 2002; Spitzberg and Hoobler 2002; Sheridan et al. 2003; Cupach and Spitzberg 2004; Purcell et al. 2004). The impact of the online context is not constant across relationship types, since this data fails

to identify any differences in case outcomes for friendships and acquaintances across the online and offline contexts studied. The online versus offline context is the stronger of the effects observed with this data.

Table 18: Summary of Hypothesized Results

	Hypothesis	Result	Statistic *Sig.*
H1	Interaction exists between relationship context and intimacy level exists in cyberstalking cases.	Supported	F = 3.279 *0.038*
H1A	Offline intimate relationships will be more severe than online intimate relationships.	Supported	MD = 0.091 *0.010*
H1B	Offline relationships with friends and acquaintances will NOT be different from online relationships with friends and acquaintances.	Supported	MD = 0.035 *0.299*
H1C	Offline relationships with strangers will be different than online relationships with strangers.	Not Supported*	MD = 0.172 *0.153*
H2	Relationship intimacy level is positively associated with severity.	Supported	F = 4.493 *0.011*
H3	Offline relationships will be more severe than online relationships.	Supported	F = 16.481 *< 0.001*
H4	Anonymity is positively associated with case severity.	Not Supported	F = 0.801 *0.525*
H5	Use of verbal media in a case will be more severe than cases using only text media.	Supported	F = 6.525 *0.002*
H6	Use of real time media in a case will be more severe than cases using only delayed media.	Not Supported	F = 3.183** *0.042*
H7	Use of private media in a case will be more severe than cases using only public media.	Not Supported	F = 0.492 *0.131*

*There was insufficient data for a meaningful result, and no conclusions should be drawn from this result.
**While the test showed significance, the direction of the result was not as postulated.

This result may also mean that online relationships are simply not as intimate as offline cases are, and the known link between intimacy level and case severity in the offline context applies. While this analysis took steps to eliminate a noted bias toward offline cases, this effort may have been insufficient. Alternatively, it is possible to conclude that online stalking is simply not as effective at impacting the victim as is offline stalking, due to weaker tools or stronger defense mechanisms that can be used by the victim to protect themselves.

Next, the anonymity of the harasser was checked for its impact on case severity. The results show that this data fails to support the postulated connection between anonymity and case severity. This result is not unexpected, as there is little in the literature that suggests that anonymity has a significant role to play in stalking generally (Spitzberg 2002). The conclusion is that this research activity presents no evidence supporting anonymity as a factor in a stalker's choice of media.

In looking at the effects of CMC channel characteristics on cyberstalking cases, the results from this data set generally supported the intuitive estimate that cases involving face-to-face and phone interactions between victims and stalkers are more severe that cases involving only textual channels. This richness variable showed that cases using verbal communications (offline, phone) were more severe than purely textual cases. This finding provides partial support for the work of Koch (2004) who, building on the deep literature related to media richness theory (Daft et al. 1987; Carlson 1995; Dennis and Kinney 1998; Carlson and Zmud 1999), postulates that support for voice communications is the most important division between richer and leaner communications channels.

On the other hand, neither the interactivity variable (real time vs. delayed) nor the distribution variable (public vs. private) showed significant differences between the categories tested. From this evidence, stalking activities taken as a whole do not require particularly high levels of interactivity. This concurs with the evidence from Miller (1999a), Sheridan et al. (2001a) and others (Cupach and Spitzberg 1994; Finkelhor et al. 2000; Spitzberg 2002; Cupach and Spitzberg 2004) that immediate feedback is not required to elevate case severity associated with disjunctive relationships, and suggests

that cyberstalking tasks are not associated with high levels of dynamic complexity. Similarly, message distribution alternatives do not lead to higher cyberstalking case severity. The evidence examined here demonstrates that cyberstalking impacts generally are not affected by the choice of message distribution mechanisms. However, this data and analysis fails to test for the difference in effectiveness of specific types of activities as affected by the distribution mechanism used, which is still likely to have an impact on the communications outcome.

Should the result shown here be supported by further research, it would appear that media channel richness has a correlation with the eventual effectiveness of a message delivered by a channel. In contrast, the interactivity and the distribution technologies of the channel do not affect stalking activities. This result, while not negating the still possible impacts of interactivity and distribution, validates Te'eni's (2001) suggestion that the characteristics of a channel have an impact on the effectiveness of the message being delivered. In conclusion, this analysis of cyberstalking data provides support for Te'eni's (2001) CAMOC model and its interpretation of media richness theory. Further, the analysis provides evidence that disjunctive online relationships are different from disjunctive offline relationships only when intimacy is involved.

Implications for Researchers

For researchers studying computer mediated communications and its associated applications, this study furthers by one small step the study of media richness theory, showing that there is a clear distinction between media that can support verbal communications and media that are limited to textual communications. At the same time,

the model used here derives from Te'eni's (2001) cognitive-affective model of organizational communications, and provides some support for its conclusions about the interactions between a sender's goals, strategies, the media used, the message, and the outcome of the communications process.

On the social sciences side, and for many of the same reasons as noted above, the use of the AHP based approach taken here to calculate our dependant variable will have value among other researchers, in particular when the construct under study contains symptomatic items that can occur one or more times in a record. This study demonstrates its effectiveness when applied to measuring stalking's impact on victims, with the caveat that the resulting measure of the outcome is not a normal curve. This can easily be corrected with the use of a transformation to correct for strong skewness. In this case, the cube root of the AHP index worked very well.

Further, in the process of developing this index of case severity, the trio of experts disagreed with the general ordering of the seriousness of stalking activity types suggested by Spitzberg (2002). The experts suggest that hyper intimacy is much more serious than is suggested in the literature reviewed by Spitzberg, and that invasion, theft and vandalism is somewhat more so. This suggests that elements of the process could be used to identify the relative impacts of this type of case, and many others, leading to a better understanding of the implications of such activities and events for victims and others.

Implications for Practitioners

The approach used by this study to determine the dependant variable, cyberstalking case severity, should prove useful to practitioners. Such an approach allows

victim support or law enforcement personnel a quick method of cataloging harassment activities, which can then be easily translated into an index value representing a standardized case severity score. This measurement process uses a form of the Analytic Hierarchy Process that removes much of the subjectivity from the process, leading to an index value for each case that is largely objective, and certainly can be applied consistently across all cases. Such a score can be used to prioritize resource allocations to cases. It can also be used, once the process is fully validated and accepted, as a means of summarizing the effects of stalking and harassment on a victim for use in legal proceedings. It is even conceivable that a standardized questionnaire and scoring weights could be used to determine if a particular case of stalking is a misdemeanor, a crime, or an aggravated crime, by establishing specific levels of severity that mark the boundaries between such definitions.

Limitations

There are several limitations on the ability to generalize the results from this study. First, the data for this research came from actual field cases, and was not initially collected by the researchers. Most importantly, the case histories available were not directly taken from the inputs of the victims. Volunteer advocates working for WHOA summarized the cases in order to generate simple statistics for publicity and tracking purposes, and it is this summary information about each case that has been used in this study. There were substantial differences in the quality of the data as provided by the different advocates, and this led to difficulties in coding, most specifically in the variables used to calculate the dependant severity variable.

Coding of the data also identified a lack of data in three of the eight cells shown in Table 1 on page 20. The three empty cells are the delayed verbal private cell, the delayed verbal public cell, and the real time verbal public cell. At this time, there are no known applications that fit the real time verbal public cell, especially since a pure form appears impractical. In practice, all large public forums utilize various control techniques to allow only selected speakers to be heard, making them appear more like broadcasting, and limiting the opportunity for the occurrence of harassment. Both the delayed verbal private and delayed verbal public cells appeared in the WHOA data. Two cases of mentioned voice mail, and one case mentioned slander via a radio broadcast. The lack of voice mail in the data is most likely related to its tight coupling to the telephone, leading to its mischaracterization by WHOA volunteers as real time phone contact. YouTube failed to appear, most likely due to its late introduction (in February 2005) relative to the period covered by the WHOA data (2001-2005). With respect to the research results presented here, there is no expectation that inclusion of reasonable numbers of cases fitting into these three cells will substantially alter the conclusions made here.

Areas for Further Research

Capturing information about the duration of a relationship prior to its conversion into a stalking case will allow a test of Carlson and Zmud's (1999) channel expansion theory, using the same techniques used in this study. WHOA has been working to improve their data collection techniques, specifically by capturing the victim's reports directly into a database, so that such a study might become possible. Additionally, this may allow the errors introduced by the advocates in the current data to be eliminated, and

allow access to information that has not been captured in the summaries to date. Access to the victim's report will allow the exploration of a variety of additional factors associated with cyberstalking, including case duration and better information on the identity and anonymity of the stalker, and will lead to an enhanced analysis of a number of the postulated effects studied in this project.

Conclusions

This research activity has proposed and used a novel and objective approach to measuring stalking case severity, and applied it to a substantial database of cyberstalking cases to good effect. The analysis of this data provides some support for the original hypothesis that offline cases would be more severe than online cases, and showed that severity is at least partly related to the type of relationship between stalker and victim prior to the initiation of the harassment. Further, there is some evidence that the richness of the media used has an impact on the outcome, namely that cases of cyberstalking are more severe when media supporting verbal communications are used.

The implications are then that there are only some differences in the impact of a specific communications media characteristics on cyberstalking severity. Based on this, this study of cyberstalking supports the general aspects of Daft and Lengel's (1986) media richness theory and the broader cogitative-affective model of organizational behavior developed by Te'eni (2001), but fails to find distinctions between a variety of CMC channels within the broader media richness model. Similarly, the results support Kock's (2004) psychobiological model of communications, which postulates a difference between media that can support speech, and those that cannot. However this study fails to

find any significant differences in the capability of various CMC media to transmit persuasive messages high in cognitive and affective content. Thus, this research supports the premise of media richness theory that face-to-face communications is richer than phone, which is in turn richer than CMC media that is based on text communications.

REFERENCES

Adams, Dennis A., Peter A. Todd and R. Ryan Nelson (1993). "A comparative evaluation of the impact of electronic and voice mail on organizational communication." *Information & Management* **24**(1): 9-21.

Aggarwal, S., M. Burmester, P. Henry, L. Kermes and J. Mulholland (2005). "Anti-cyberstalking: the Predator and Prey Alert (PAPA) system." *First International Workshop on Systematic Approaches to Digital Forensic Engineering, 2005*, IEEE.

Alexy, Eileen M., Ann W. Burgess, Timothy Baker and Shirley A. Smoyak (2005). "Perceptions of Cyberstalking Among College Students." *Brief Treat Crisis Intervention* **5**(3): 279-289.

Bargh, John A. (2002). "Beyond Simple Truths: The Human-Internet Interaction." *Journal of Social Issues* **58**(1): 1-8.

Bargh, John A., Katelyn Y. A. McKenna and Grainne M. Fitzsimons (2002). "Can You See the Real Me? Activation and Expression of the "True Self" on the Internet." *Journal of Social Issues* **58**(1): 33-48.

Beran, Tanya and Li Qing (2005). "Cyber-Harassment: a Study of a New Method for an Old Behavior." *Journal of Educational Computing Research* **32**(3): 265-277.

Berthold, Oliver, Hannes Federrath and Marit Köhntopp (2000). "Project “anonymity and unobservability in the Internet”." *Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions*, Toronto ON, ACM Press New York, NY, USA.

Birtchnell, John (1993). *How Humans Relate: A New Interpersonal Theory*. Westport, Conn., Praeger.

Bocij, Paul (2004). *Cyberstalking : harassment in the Internet age and how to protect your family*. Westport, Conn., Praeger.

Brenner, Susan W. (2004). "U.S. Cybercrime Law: Defining Offenses." *Information Systems Frontiers* **6**(2): 115-132.

Brewster, M. P. (2000). "Stalking by former intimates: verbal threats and other predictors of physical violence." *Violence and Victims* **15**(1): 41-54.

Carlson, John R. and Robert W. Zmud (1999). "Channel Expansion Theory and the Experiential Nature of Media Richness Perceptions." *Academy of Management Journal* **42**(2): 153-170.

Carlson, John Ross (1995). Channel expansion theory: A dynamic view of media and information richness perceptions. *ProQuest Dissertations and Theses*. Tallahassee FL, Florida State University. **Ph.D:** 178 p.

Connolly, Terry, Leonard M. Jessup and Joseph S. Valacich (1990). "Effects of Anonymity and Evaluative Tone on Idea Generation in Computer-Mediated Groups." *Management Science* **36**(6): 689.

Cupach, William R. and Brian H. Spitzberg (1994). *The Dark side of interpersonal communication*. Hillsdale, N.J., L. Erlbaum.

Cupach, William R. and Brian H. Spitzberg (1998). Obsessive relational intrusions and stalking. *The dark side of close relationships*. Brian H. Spitzberg and William R. Cupach. Mahwah, NJ, Lawrence Erlbaum**:** 233-263.

Cupach, William R. and Brian H. Spitzberg (2000). "Obsessive relational intrusion: Incidence, perceived severity and coping." *Violence and Victims* **15**(4): 357-372.

Cupach, William R. and Brian H. Spitzberg (2004). *The Dark Side of Relationship Pursuit: From Attraction to Obsession and Stalking*. Mahwah, N.J., Lawrence Erlbaum Associates.

D'Ovidio, Robert and James Doyle (2003). "A Study on Cyberstalking Understanding Investigative Hurdles." *FBI Law Enforcement Bulletin* **72**(3): 10-17.

Daft, Richard L. and Robert H. Lengel (1986). "Organizational Information Requirements, Media Richness and Structural Design." *Management Science* **32**(5): 554.

Daft, Richard L., Robert H. Lengel and Linda Klebe Trevino (1987). "Message Equivocality, Media Selection, and Manager Performance: Implications for Information Systems." *MIS Quarterly* **11**(3): 355.

Dennis, Alan R. and Susan T. Kinney (1998). "Testing media richness theory in the new media: The effects of cues, feedback, and task equivocality." *Information Systems Research* **9**(3): 256-274.

Dennis, Alan R., Susan T. Kinney and Yu-Ting Caisy Hung (1999). "Gender Differences in the Effects of Media Richness." *Small Group Research* **30**(4): 405-437.

Dennis, Alan R., Barbara H. Wixom and Robert J. Vandenberg (2001). "Understanding Fit and Appropriation Effects in Group Support Systems via Meta-analysis." *MIS Quarterly* **25**(2): 167-194.

Dziegielewski, Sophia and Albert R. Roberts (1995). Stalking Victims and survivors: Identification, legal remedies and crisis treatment. *Crisis intervention and time-limited cognitive treatment*. Albert R. Roberts. Thousand Oaks, Sage Publications**:** 73-90.

Ellison, Louise and Yaman Akdeniz. (1998). "Cyber-stalking: the Regulation of Harassment on the Internet." *Criminal Law Review* Retrieved May 23, 2006, from http://www.cyber-rights.org/documents/stalking_article.pdf.

Emerson, Robert M., Kerry O. Ferris and Carol Brooks Gardner (1998). "On Being Stalked." *Social Problems* **45**(3): 289-314.

Finch, Emily (2001). *The Criminalisation of Stalking: Constructing the Problem and Evaluating the Solution*. London, Cavendish.

Finkelhor, David, Kimberly J. Mitchell and Janis Wolak. (2000). *Online Victimization: A Report on the Nation's Youth*. (98-MC-CX-K002). Alexandria VA: National Center for Missing and Exploited Children. 60 pgs.

Finn, Jerry (2004). "A Survey of Online Harassment at a University Campus." *Journal of Interpersonal Violence* **19**(4): 468-483.

Fisher, Bonnie S., Francis T. Cullen and Michael G. Turner. (2000). *The Sexual Victimization of College Women*. (NCJ 182369). Washington DC: US Department of Justice, National Institute of Justice. 47 pgs.

Fremouw, William J., Darah Westrup and Jennifer Pennypacker (1997). "Stalking on campus: the prevalence and strategies for coping with stalking." *Journal of Forensic Sciences* **42**(4): 666-669.

Freund, Rudolf Jakob and William J. Wilson (2003). *Statistical Methods* 2nd ed. San Diego, Calif., Academic Press.

Glaser, Jack, Jay Dixit and Donald P. Green (2002). "Studying Hate Crime with the Internet: What Makes Racists Advocate Racial Violence?" *Journal of Social Issues* **58**(1): 177-193.

Glaser, R. (1983). *The corporate culture survey*. Byrn Mawr, PA, Organizational Design and Development.

Goldberg, D and V. F. Hillier (1979). "A Scaled Version of the General Health Questionnaire." *Psychological Medicine* **9**: 139-145.

Goldberg, D. P., R. Gater, N. Sartorius, T. B. Ustun, M. Piccinelli, O. Gureje and C. Rutter (1997). "The validity of two versions of the GHQ in the WHO study of mental illness in general health care." *Psychological Medicine* **27**(01): 191-197.

Goode, Mathew (1995). "Stalking: The Crime of the Nineties?" *Criminal Law Journal* **19**(1): 215-234.

Habermas, Jèurgen (1984). *The theory of communicative action*. Boston, Beacon Press.

Habermas, Jèurgen and Maeve Cooke (1998). *On the pragmatics of communication*. Cambridge, Mass., MIT Press.

Hair, Joseph F., Rolph E. Anderson, Ronald L. Tatham and William C. Black (1998). *Multivariate Data Analysis* 5th ed. Upper Saddle River, N.J., Prentice Hall.

Harmon, Ronnie B., Richard Rosner and Howard Owens (1995). "Obsessional harassment and erotomania in a criminal court population." *Journal of Forensic Sciences* **40**(2): 188-196.

Heinlein, Robert A. (1966). *The Moon is a Harsh Mistress*. New York, Putnam.

Hian, Lee Bee, Sim Li Chuan, Tan Mon Kiat Trevor and Benjamin H. Detenber (2004). "Getting to know you: exploring the development of relational intimacy in computer-mediated communication." *Journal of Computer-Mediated Communication* **9**(3).

Horowitz, M., N. Wilner and W. Alvarez (1979). "Impact of Event Scale: A Measure of Subjective Stress." *Psychosomatic Medicine* **41**: 209-218.

Kock, Ned (2004). "The Psychobiological Model: Towards a New Theory of Computer-Mediated Communication Based on Darwinian Evolution." *Organization Science* **15**(3): 327.

Kraut, Robert, Sara Kiesler, Bonka Boneva, Jonathon Cummings, Vicki Helgeson and Anne Crawford (2002). "Internet Paradox Revisited." *Journal of Social Issues* **58**(1): 49-74.

Lee, Heeseok, Yong Shi, Sufi M. Nazem, Sung Yeol Kang, Tae Ho Park and Myung Ho Sohn (2001). "Multicriteria hub decision making for rural area telecommunication networks." *European Journal of Operational Research* **133**(3): 483-495.

Lewis, Clive Staples (1960). *The Four Loves*. New York,, Harcourt.

Lubatkin, Michael H. , Momar Ndiaye and Richard Vengroff (1997). "The nature of managerial work in developing countries: A limited test of the universalist hypothesis." *Journal of International Business Studies* **28**(4): 711.

McCann, Joseph T. (2001). *Stalking in children and adults : the primitive bond* 1st ed. Washington, DC, American Psychological Association.

McKenna, Katelyn Y. A., Amie S. Green and Marci E. J. Gleason (2002). "Relationship Formation on the Internet: What's the Big Attraction?" *Journal of Social Issues* **58**(1): 9-31.

McLaughlin, Margaret L. (1984). *Conversation: How Talk is Organized*. Beverly Hills, Sage Publications.

Meloy, J. Reid (1998). *The psychology of stalking: clinical and forensic perspectives*. San Diego, Academic Press.

Miceli, Sharon Levrant, Shannon A. Santana and Bonnie S. Fisher (2001). "Cyberaggression: Safety and Security Issues for Women Worldwide." *Security Journal* **14**(2): 11-27.

Miller, Greg (1999a). Chilling Cyber-Stalking Case Illustrates New Breed of Crime. *Los Angles Times*. Los Angles CA**:** 1.

Miller, Greg (1999b). N. Hollywood Man Charged in 1st Cyber-Stalking Case. *Los Angles Times*. Los Angles, CA**:** 1.

Mohandie, Kris, J. Reid Meloy, Mila Green McGowan and Jenn Williams (2006). "The RECON Typology of Stalking: Reliability and Validity Based Upon a Large Sample of North American Stalkers." *Journal of Forensic Sciences* **51**(1): 147-155.

Mullen, Paul E., Michele Pathé and Rosemary Purcell (2000). *Stalkers and their victims*. Cambridge, U.K. ; New York, Cambridge University Press.

Mullen, Paul E., Michele Pathé, Rosemary Purcell and Geoffrey W. Stuart (1999). "Study of Stalkers." *American Journal of Psychiatry* **156**(8): 1244-1249.

Pathe, Michele and Paul E. Mullen (1997). "The impact of stalkers on their victims." *British Journal of Psychiatry*.

Pedhazur, Elazar J. and Liora Pedhazur Schmelkin (1991). *Measurement, Design, and Analysis : An Integrated Approach*. Hillsdale, N.J., Lawrence Erlbaum Associates.

Phillips, Lorraine, Ryan Quirk, Barry Rosenfeld and Maureen O'Connor (2004). "Is it Stalking?: Perceptions of Stalking among College Undergraduates." *Criminal Justice and Behavior* **31**(1): 73-96.

Purcell, Rosemary, Michele Pathe and Paul E. Mullen (2004). "Editorial: When do repeated intrusions become stalking?" *Journal of Forensic Psychiatry and Psychology* **15**(4): 571-583.

Roberts, Albert R. and Sophia F. Dziegielewski (2006). "Changing Stalking Patterns and Prosecutorial Decisions: Bridging the Present to the Future." *Victims & Offenders* **1**(1): 47-60.

Rosenfeld, Barry (2004). "Violence Risk Factors in Stalking and Obsessional Harassment: A Review and Preliminary Meta-Analysis." *Criminal Justice and Behavior* **31**(1): 9-36.

Roth, Kendall and Allen J. Morrison (1990). "An Empirical Analysis of the Integration-Responsiveness Framework in Global Industries." *Journal of International Business Studies* **21**(4): 541.

Saaty, Thomas L. (1994). *Fundamentals of decision making and prority theory with the analytic hierarchy process* 1st ed. Pittsburgh, PA, RWS Publications.

Saaty, Thomas L. and Luis G. Vargas (2001). *Models, methods, concepts & applications of the analytic hierarchy process*. Boston, Kluwer Academic Publishers.

Sheridan, Lorraine, Graham Davies and Julian Boon (2001a). "The Course and Nature of Stalking: A Victim Perspective." *The Howard Journal* **40**(3): 215-234.

Sheridan, Lorraine, Graham Davies and Julian Boon (2001b). "Stalking: Perceptions and Prevalence." *Journal of Interpersonal Violence* **16**: 151-167.

Sheridan, Lorraine, Raphael Gillett and Graham Davies (2002). "Perceptions and Prevalence of Stalking in a Male Sample." *Psychology, Crime and Law* **8**(4): 289-310.

Sheridan, Lorraine P., Eric Blaauw and Graham M. Davies (2003). "Stalking: Knowns and Unknowns." *Trauma Violence Abuse* **4**(2): 148-162.

Snodgrass, J. Josh, William R. Leonard, Mark V. Sorensen, Larissa A. Tarskaia, Vasili P. Alekseev and Vadim Krivoshapkin (2006). "The Emergence of Obesity among Indigenous Siberians." *Journal of Physiological Anthropology* **25**(1): 75-84.

Spears, Russell, Tom Postmes, Martin Lea and Anka Wolbert (2002). "When Are Net Effects Gross Products? Communication." *Journal of Social Issues* **58**(1): 91-107.

Spitzberg, Brian H. (2002). "The Tactical Topography of Stalking Victimization and Management." *Trauma Violence Abuse* **3**(4): 261-288.

Spitzberg, Brian H. and William R. Cupach, Eds. (1998). *The dark side of close relationships*. Mahwah, N.J., Lawrence Erlbaum.

Spitzberg, Brian H. and Greg Hoobler (2002). "Cyberstalking and the technologies of interpersonal terrorism." *New Media Society* **4**(1): 71-92.

Straub, Detmar and Elena Karahanna (1998). "Knowledge worker communications and recipient availability: Toward a task closure explanation of media choice." *Organization Science* **9**(2): 160-175.

Taylor, Bernard W. (2004). *Introduction to Management Science* 8th ed. Upper Saddle River NJ, Pearson Prentice Hall.

Te'eni, Dov (2001). "Review: A Cognitive-Affective Model of Organizational Communication for Designing IT." *MIS Quarterly* **25**(2): 251-312.

Thompson, Leigh and Janice Nadler (2002). "Negotiating via Information Technology: Theory and Application." *Journal of Social Issues* **58**(1): 109-124.

Tjaden, Patricia Goedeke and Nancy Thoennes. (1998). *Stalking in America: findings from the National Violence Against Women Survey*. (NCJ 169592). Washington, DC: National Institute of Justice and Centers for Disease Control and Prevention. 19 pgs.

Tjaden, Patricia Goedeke and Nancy Thoennes. (2000). *Full Report of the Prevalence, Incidence, and Consequences of Violence Against Women: Findings From the National Violence Against Women Survey*. (NCJ 183781). Washington DC: US Department of Justice, National Institute of Justice. 74 pgs.

Tyler, Tom R. (2002). "Is the Internet Changing Social Life? It Seems the More Things Change, the More They Stay the Same." *Journal of Social Issues* **58**(1): 195-205.

Walther, Joseph B. (1996). "Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction." *Communication Research* **23**(1): 3-43.

WHOA. (2006). "Working to Halt Abuse Online." Retrieved April 26, 2006, from http://www.haltabuse.org/index.shtml.

Zigurs, Iize and Bonnie K. Buckland (1998). "A theory of task/technology fit and group support systems effectiveness." *MIS Quarterly* **22**(3): 313-334.

Zona, Michael A., Kaushal K. Sharma and John Lane (1993). "A comparative study of erotomanic and obsessional subjects in a forensic sample." *Journal of Forensic Sciences* **38**(4): 894-903.

APPENDIX A:

CODING GUIDELINES FOR CYBERSTALKING DATA

Project Objectives

Recent research is showing that the Internet is having an impact on interpersonal relationships, often accelerating their development (Bargh et al. 2002; McKenna et al. 2002), and in some cases, accentuating the problems (Thompson and Nadler 2002). One subset of interpersonal relationships includes those that fail to share a common goal between parties. One group of researchers labels this type of relationship as a disjunctive relationship (Cupach and Spitzberg 2004). When interpersonal relations break down, usually when one party decides to break up the relationship, a disjunctive relationship results. Until both parties accept the eventual outcome, the relationship remains in this disjunctive state. Disjunctive relationships are characterized by ongoing conflict, often taking the form of modest harassment, and occasionally leading to more severe extremes such as stalking. Online harassment and stalking are known as cyberstalking.

This project is interested in the impacts of the Internet on stalking and harassment. Specifically, it studies the impact of the internetworking technologies on case severity. To that end, I have acquired five years of case histories of cyberstalking incidents from an online victims support group. Two main elements of this data are relevant to the research, the nature of the relationship between the parties before and during the harassment (the independent variables), and severity of the case (the dependant variable).

A third element of the data is postulated to act as a moderator: the characteristics of the communications technology used by the parties to the case.

Nature of the Source Data

Data comes from Working to Halt Online Abuse (WHOA), a volunteer organization that helps victims of online harassment identify their harasser and aids in the resolution of cases when their technology skills are needed. WHOA provides referrals to law enforcement and other agencies when the case merits such attention, and will assist such groups when necessary. In return, these agencies often refer less severe cases to WHOA and similar groups. WHOA's case histories were not captured for use in extensive analysis and need significant recoding to be useful. A first pass examination provided the basis for the coding standards that are described below. The same first pass also took care of simple and objective items such as age, gender and race of the victim.

Additional Directions

The order of the data rows has been uniquely randomized for each coder to minimize the effects of coder experience as they work through the data file. Please do not reorder the file, or add or delete rows or columns. This will aid in reordering the file for evaluation of inter-rater reliability and overall analysis.

The Moderator Variables

The first pass coding of the data identified some 40 techniques for using electronic communications to harass or stalk the victim. 13 of these appeared more than

20 times in the data, and are identified in the common tool column in Table A1 below. The remainder occurred less than 10 times in the initial coding.

Table A1: Internet Communications Tools & Techniques

Common Tools	Uncommon Tools	Unique Tools
Email	Trojan Horse Software	False Report to Authorities
Instant Messaging	Posting of Pictures	False Profile
Message Boards	Proxy Complaint	Forged Account
Phone	Identity Research	Paging
Website	Viruses Attempted	IP Theft
Chat	Web Cameras	Radio & Media
Offline	Fax	SMS
Listserves	E-cards	Spoofing
Postal Mail	Hijacked Email	Stalking
Ebay	Directed Spam	Subscribe to Groups
Blogs	Spyware	Unwanted Subscriptions
Usenet	Wikipedia	Web rings
Hacking		
Game Forums		

Note that several non-Internet tools are included here, including postal mail, phone, fax, and others. These also provide value for this study, and should be captured accordingly. Cases that include physical contact, aggression or other activities that require physical contact or proximity should note this by setting the "Offline" value in addition to any other values identified.

Coding Online Media Used in the Case

The first coding item is the media tool used for the first harassing message. For the common tools, code the tool name (e.g. Email). For uncommon and unique tools, code "Other" and be sure the tool is coded in the "other media type" column. If none at all are identified, mark the case as "Unspecified."

To code the media moderators, we take a symptomatic approach. There are 15 columns in the data sheet, one for each common media type, plus "offline" and "other." Code a "1" in a column if that media type is mentioned anywhere in the data for a given

case, “0” otherwise. (Do not code for any communications with WHOA, code only the communications between the victim and harasser.) Code every tool type mentioned. If any of the uncommon or unique tools are mentioned, code a “1” in the “other” column and note the tool type(s) in the adjacent “other media type” column. If, in your opinion, you identify a new tool type here, please added it to the “other media type” column, and make a note of it for my use later. If none at all are identified, mark all the tool columns “0” for not used.

The Independent Variables

There are three independent variables that are postulated to affect the severity of a cyberstalking case, the nature and intensity level of the relationship, anonymity of the perpetrator, and the locus of the context of the relationship, e.g. did the relationship exist online or offline.

Coding the Nature of the Relationship

Offline stalking identifies a correlation between the nature of the relationship between the victim and the harasser. Generally, the closer the prior relationship between the parties, the more severe is the impact on the victim. The labels provided in Table A2 should be used to capture the nature of the relationship:

Table A2: Relationship Intimacy Levels

Spouse	Current or former spouse
Intimate	Current or former intimate; girlfriend; boyfriend; implies mutual effort by the parties to establish a relationship with a "significant other."
Friend	Friend or confidant; not intimate, but close and implies a mutual commitment to the relationship
Acquaintance	Someone known to the victim in a casual or professional setting; classmate; coworker; manager; service provider. Includes friends of friends and former partners of current intimates or spouses.
Family	Any member of the victims extended family, including family of current or former partners, but excluding current or former partners.
Unknown	Strangers and others when the true identity is unknown to the victim.

Coding for Anonymity

The Internet provides useful capabilities for individuals to hide their true identity from others. Harassers can use this to induce fear in their victims. To see if this has a real impact in online circumstances, we need to code the case for the likely anonymity of the harasser. Because identities can be discovered, we use the beginning of the harassing acts as the point in time to determine if the harasser is attempting to maintain anonymity. Use the codes identified in Table A3 to code for anonymity.

Table A3: Anonymity Codes

Anonymous	When the true identity of the perpetrator is unknown to the victim when the harassment began.
Not Anonymous	When the true identity of the perpetrator is clearly known to the victim when the harassment began.
Unknown	Cases where anonymity cannot be determined from the information available in the case record.

Note that strangers are different from anonymous stalkers. A stranger is someone unknown to the victim, but who does not try to hide their identity. An anonymous stalker may be a stranger, but may also be a former intimate, friend or family member. The latter seeks to hide their true identity from the victim, while the former does not.

Coding for Relationship Context & Evolution

In our research, we are seeking to understand if the context of the relationship has an impact on the eventual severity of the case. We are interested in two loci, whether the relationship exists online or offline. In some cases, online cases move offline as the relationship evolves, and we can use this information as well. This information is not clearly identified in the source data, and must be derived from the case content. Use the labels in Table A4 to capture the context of the relationship:

Table A4: Context of Relationship

Online	Originally and still purely online. The parties have never met face to face.
Offline	The parties originated the relationship using traditional means offline, but the harassment included online activities.
On2Off	A relationship that began online, but moved offline over time. This will not be common. Cases where the harassment began well after the relationship moved offline should be coded "Offline."
Unknown	Cases where there is insufficient data to determine the context of the relationship. These cases will be excluded from portions of the analysis.

The Dependant Variable Components

Stalking always consists of multiple acts that the victim perceives as threatening. To measure the seriousness or severity of each case, we take a symptomatic approach, and then apply the Analytic Hierarchy Process to determine weights for each symptom identified, which are then summated case by case into a severity score. This relies on binary coding for the presence (or not) of a particular type of action as recorded in the case history. In order to make the resulting severity score more reliable, we are coding each case in three domains: the presence of threats to the victim, actions taken by the perpetrator against the victim, and information about the eventual result of the case.

Coding Threat Information

To code the threat information, we take a symptomatic approach. There are 6 columns in the data sheet, one for each threat type identified below, plus "no threats." Code a "1" in a column if that threat type is mentioned anywhere in the data for a given case, "0" otherwise. This approach allows us to identify if multiple different types of threats were recorded in each case. Table A5 defines each of the threat types, and is derived in part from (Spitzberg 2002).

Table A5: Codes for Threat Information

Information Release	Disclosure of personal information; Outing; Blackmail.
Other threats (unspecified)	General threats; Emotional threats; Self harm; Suicide; Threatening calls/letters/gifts/messages.
Property Damage	Threats against property or other tangibles; Threats to hack computers, hijack email, etc.; Threatened or actual theft of property; Breaking & entering.
Friend, family or pets	Specific threats against friends, family, or pets; Verbal threats about partners, loved ones.
Death threats	Specific verbal or written death threats; Strong threats of violence towards victim; Threaten with a weapon.
No threats	No threats were identified in the case data

Coding Action Information

Stalking is a series of actions that together induce fear in the victim. By themselves, these actions may not be a cause for concern. Thus we again take a symptomatic approach. There are 11 columns in the data sheet, one for each action type identified below, plus "no actions." Code a "1" in a column if that action type is mentioned anywhere in the data for a given case, "0" otherwise. This approach allows us to identify if multiple different types of actions were recorded in each case. Table A6 defines each of the action types, and is derived in part from (Spitzberg 2002).

Table A6: Codes for Action Information

Courtship behaviors	Engaging target as a stranger in unsolicited conversation in a public place; Offering to by a drink in a public place as a stranger.
Overbearing or Obscene Actions	Making obscene comments as a stranger; Asking for a date more than once after being refused.
Impersonation	Using the victim's identity to make obnoxious or worse statements about others; Making offers on the victim's behalf.
Hacking, Trojans, spyware, etc.	Misuse of computer networks to steal information; spy on the victim's actions, or damage victim's computer.
Hyperintimacy	Excessive courtship behaviors; Excessive communications attempts; many unwanted gifts.
Pursuit, Proximity, & Surveillance	Lying in wait; Synchronizing activities; Unauthorized photos; Following; Drive-bys.
Invasion, Theft, Vandalism	Property invasion; Information theft; Property theft or damage.
Proxy Pursuit & Intrusion	Involve 3rd Parties for information gathering or proximity opportunities; Intimidate via intermediaries.
Intimidation, Slander, & False Charges	Includes Sabotage and Reputational Harassment; Blackmail; Threats of disclosure to employer; Making false claims to CPS.
Coercion & Constraint	Extortion; Use of physical force; Kidnapping.
Aggression	Assault on property, pets, self, or others; Violence towards victim; Rape; Endangerment.

In addition, there are two action columns for "No Action Data in Case" and "Was Not Harassment." Use the first if the case is identified as a harassment case, but no action information is identifiable. Use the latter if the case was not harassment. Mostly, this will consist of "Spam", along with a few other cases. Cases marked "Was Not Harassment" will be deleted from the database before any analysis is undertaken.

Coding Result Information

Table A7 captures most of the outcomes of cases, where known. Identify the outcome of the case. If several items on this list are mentioned, code the most severe. The list is ordered in severity from least (top) to most severe (bottom). For items not appearing here, code the case as "Other: < type>", replacing the <type> field to capture a

brief description of the outcome. For example: for a case might be coded “Other: Removed spyware”.

Table A7: Codes for Result Information

Advice Ignored	Victim ignored WHOA advice; Also 2 way fights; Flame wars; Reporting party is part of problem.
Harassment Ended	Harassment ended after brief time.
Material Removed	Offending materials removed from web/blog/etc.
Stopped Using Service	Victim stopped using service; Avoided list/chat room/blog.
Changed Online Identity	Victim changed online identity; New email address; New chat room handles.
Reported to ISP	Victim or WHOA reported to ISP for action.
ISP Banned Harasser	The ISP hosting the service banned the harasser; Harasser’s accounts closed.
Referred to Attorney	Victim referred to Attorney for legal action or follow-up.
Referred to Law Enforcement	Victim referred to law enforcement for legal action.
Restraining Order	Victim advised to obtain a restraining order, or has had one issued against harasser.
Charges Pending	Harasser has charges pending related to this case.
Other Outcomes	All other diverse outcomes, as “Other: <type>”
Unknown	The WHOA data provides no information about outcome, and all cases that are not harassment or stalking.

APPENDIX B:

USE OF THE ANALYTIC HIERARCHY PROCESS

In developing this research, it was necessary to identify and use an objective function for assigning a numerical severity score to each cyberstalking case. The inputs available included information on types of harassing acts, threats, and results that could be coded as present or not for each case. By establishing weights for each type of act and threat, the sum of the weights for acts and threats present in a case can be used as the severity score. What is required is a method for generating weights for each type of harassing act, threat, and case result found in the data. The Analytic Hierarchy Process (AHP) developed by Saaty and Vargas (Saaty 1994; Saaty and Vargas 2001) provides a mechanism for the production of such weights, among other uses. For example, Lee et al. (2001) use AHP as a means of determining criterion weights associated with a telecommunications network design problem, similar to the problem here.

AHP originated in the decision sciences discipline as an approach valuable for the rational evaluation of pros and cons concerning different alternative solutions. When used to make decisions, AHP answers the question "Which one?" (Taylor 2004). The useful feature of AHP in this study is order ranking and weight assignment for each of the input alternatives. This can be accomplished using inputs from one or a very small number of subject matter experts knowledgeable in the relevant domain of interest.

In this study, these weights are used to calculate the severity score for each case. Taylor's (2004 p372) spreadsheet implementation of AHP was used to generate weights for each item in the three separate data types in the case histories: harassing activities, threats, and case results. These weights are presented in Tables 8-10 in Chapter IV. The AHP process was repeated to establish relative weights for the three type areas (acts, threats, and results), generating the AHP weights given in Tables 11 in Chapter IV.

Using AHP to Get Objective Item Weights

The general mathematical process involved in AHP (when used as a decision tool) is to establish preference weights for each of the criterion (the higher level), and to establish preference weights for each alternative within each criterion area (the lower level). If needed, additional levels can be used to extend the technique to sub-groups of criteria (Taylor 2004).

AHP begins by listing and defining the criterion and alternatives. In this case, we based the lists of harassing acts and threats on the work of Spitzberg (2002) as shown in Tables 8 and 9 in Chapter IV. A separate list of results was derived from the data, condensed into a smaller number of types, and is shown in Table 10 in Chapter IV. Each item was defined for use in a pair-wise comparison survey instrument, a copy of which is included in Appendix C. AHP uses a standard preference scale where the rater chooses values on a scale to describe a preference for one item over the other. This was modified for use in this study, to ask for the difference in severity of an act or threat, from the perspective of the victim and/or the criminal justice system. Table B1 identifies the

severity difference levels used in this activity, with the intermediate levels provided, but not named, on the survey instrument.

Table B1: AHP Severity Difference Scale

Severity Difference Level	Numerical Value
Equally Severe	1
Somewhat More Severe	3
Significantly More Severe	5
Substantially More Severe	7
Extremely More Severe	9

The survey instrument, which appears in Appendix C, was distributed to a trio of professionals currently working in the domestic violence field. Their task was to estimate the difference in severity between pairs of activities, and pairs of threats. The trio of respondents included an investigative detective from a large metropolitan police force specializing in stalking and domestic abuse cases, and two members of a coordinating council on domestic violence serving the same metropolitan area. Inter-rater reliability for the three respondents was $\alpha = 0.820$. The results of this survey were averaged item by item per Saaty (1994) and used as inputs into the next step of the AHP process. A less formal dialog was used to obtain inputs for the case results category with the staff at WHOA, identifying the severity difference levels for each pair of result types.

Taylor (2004) presents AHP in a form suitable for calculation using spreadsheets. Using this method, the pair-wise severity difference levels were input into a pair-wise comparison matrix. This is a square matrix, with the survey's averaged difference levels entered into the matrix array. When the row item is more severe than the column item, the difference level is entered. When the column item is more severe than the row item, the reciprocal of the difference level is entered into the matrix. The diagonal is filled with

value of 1.00 to show equality of the row and column. Table B2 shows this information for the threat items used in this study.

Table B2: AHP Threat Comparison Matrix

Raw Score	TIR	TP	OT	FFP	DT
Threaten Information Release	1.00	2.00	0.23	0.14	0.12
Threaten Property	0.50	1.00	0.23	0.17	0.13
Other Threats	4.33	4.33	1.00	0.25	0.19
Threaten Friends, Family or Pets	7.00	6.00	4.00	1.00	1.00
Death Threats	8.33	7.67	5.33	1.00	1.00
Sum	**21.17**	**21.00**	**10.79**	**2.56**	**2.44**

How much more severe is the ROW over the COLUMN?

The columns of this matrix are summed, and each element of the matrix is normalized by dividing every element by the sum of its respective column. Table B3 shows the results of this process for threat items used in this study. Next, each row in the matrix is averaged. These averages are the weights attached to the (row) item, and make up the weighting vector necessary for this study.

Table B3: AHP Normalized Threat Matrix

Raw Score	TIR	TP	OT	FFP	DT	Row Average
Threaten Information Release	0.05	0.10	0.02	0.06	0.05	**0.054**
Threaten Property	0.02	0.05	0.02	0.07	0.05	**0.042**
Other Threats	0.20	0.21	0.09	0.10	0.08	**0.136**
Threaten Friends, Family or Pets	0.33	0.29	0.37	0.39	0.41	**0.358**
Death Threats	0.39	0.37	0.49	0.39	0.41	**0.411**

The output can be thought of as the distance between the items as spread out on a linear scale, with an overall range of zero to one, since the sum of the weights will always equal one. The same process was used to obtain weights for the list of harassing acts, the case result items, and weights for the overall factors of harassing acts vs. threats vs. results, as shown in Table 11 in Chapter IV.

Because the inputs to this process are subject to human error and inconsistency, a consistency check process has been developed (Taylor 2004 p379-380). To measure consistency, the comparison matrix is multiplied by the weighting vector, with the resulting values divided by the weighting vector and averaged. The resulting average is used to compute a consistency index (CI) using the formula $CI = (Average - n)/(n - 1)$, where n is the number of items. If the CI equals zero, the inputs are perfectly consistent. More commonly, this is not the case, and Taylor (2004) provides a series of random indices (RI), one for each n, that have been calculated using randomly generated pair-wise comparisons. The CI is divided by the RI. The resulting value should be less than 0.10 to show that the inputs are reasonably consistent. The consistency check values for the items of interest here are shown in Table B4.

Table B4: AHP Consistency Check Values

Severity Factor	Consistency Check Value
Activities	0.071
Threats	0.058
Results	0.072
Overall Factors	0.016

Using AHP Derived Weights to Calculate Case Severity Scores

To develop the index of case severity, WHOA case data is scored with a Boolean value of one (or zero) showing the presence (or not) of each specific type of activity, threat, or result, respectively, within each category. An intermediate category score is calculated for each of the three categories of activities, threats, and results by multiplying the Boolean value for each item by its weight, and summing the resulting values. The three category scores are then multiplied by their factor weights and summed again, producing a single case severity score. The following equation summarizes this activity:

$$S = W_A \sum A_i A_i' + W_T \sum T_j T_j' + W_R \sum R_k R_k'$$

where

A_i = AHP weight for action type *i*, $\sum A_i = 1$, (from Table 8),

T_j = AHP weight for threat type *j*, $\sum T_j = 1$, (from Table 9),

R_k = AHP weight for result type *k*, $\sum R_k = 1$, (from Table 10),

A_i' = Boolean indicating presence of action type *i* in case,

T_j' = Boolean indicating presence of threat type *j* in case,

R_k' = Boolean indicating presence of result type *k* in case,

$W_A + W_T + W_R = 1$ = aggregate factor weights (from Table 11), and

S is the case severity score.

APPENDIX C:

QUESTIONNAIRE USED TO DEVELOP AHP WEIGHTS.

Cyberstalking Activity Severity Comparison

Research Project Goals:

Traditional stalking is defined generally as "***unwanted persistent personal harassment***." Stalking generally takes the form of a series of actions that independently may or may not be considered harassment. Cyberstalking is stalking perpetrated exclusively or largely with computer mediated communications and/or other online applications and services. In other words, using the Internet. This research project attempts to analyze records of historical cases of cyberstalking and online harassment to understand the forms that cyberstalking takes, and how the Internet has affected traditional stalking. For instance, it appears that men are victims of cyberstalking more often than would be expected, based on traditional stalking data. We want to know first if this is true, and if so, why. We also wish to determine if the Internet provides opportunities for harassment that have yet to be examined by researchers, by looking at cyberstalking case histories.

Stalking can encompass many actions. Such actions may, for instance, include sending excessive cards, letters, emails, or unwanted gifts, inappropriate physical approaches, ingratiation, surveillance, following, information theft, property invasion, theft or damage, verbal or non-verbal intimidation, reputational harassment, threats, coercion, extortion, and various forms of criminal aggression including attacking pets, assault, and rape.

Purpose of this Questionnaire:

To achieve our research goals, we need to characterize online actions that can be a part of cyberstalking as well as traditional stalking. A critical component of this is to understand the relative levels of severity represented by each stalking action type in comparison with other stalking actions. This survey will be used to measure the perceived differences in severity for paired stalking actions and threats. The resulting data will be mathematically combined with the historical data to develop a severity score for each case. That case severity score will then be used in combination with other information to inform our broader research into cyberstalking.

The specific approach we are taking for this measurement is known as Analytic Hierarchy Process (AHP). AHP allows us to determine severity weights for each category and factor in our research data. AHP depends on the input of values from a decision maker or other expert in the relevant field. Finally, we intend to combine these weights with data coded from the historical case records to get an overall severity score for each case. This will be used as a dependant variable to answer a variety of detailed research questions using statistical analysis techniques on the coded historical data.

Cyberstalking Activity Severity Comparison

Below is a list of personal threat type pairs. Each threat type can be an element of a stalking/ cyberstalking case. Using the check box, please identify which action is more severe, ***from the perspective of the victim and/or criminal justice system***. Then, using the rating scale, specify the difference in severity between the two cases by circling a number. Circle "1" if both are equal in your mind.

Definitions for Threat Categories

Threaten to release personal information	Disclosure of personal information; Outing; Blackmail.
Threaten property damage	Threats against property or other tangibles; Threats to hack computers, hijack email, etc.
Other (unspecified) threats	General threats; Verbal threats about partners, loved ones; Emotional threats.
Threaten friends, family, or pets	Specific threats against friends, family, or pets.
Verbal or written death threat	Specific verbal or written death threats.

	Threat Pairs	More Severe	Equally Severe	Somewhat More Severe	Significantly More Severe	Substantially More Severe	Extremely More Severe
1	Other (unspecified) threats Threaten to release personal information	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
2	Threaten property damage Other (unspecified) threats	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
3	Threaten friends, family, or pets Threaten property damage	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
4	Verbal or written death threat Threaten friends, family, or pets	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
5	Threaten to release personal information Threaten property damage	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
6	Other (unspecified) threats Threaten friends, family, or pets	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
7	Threaten property damage Verbal or written death threat	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
8	Threaten friends, family, or pets Threaten to release personal information	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
9	Verbal or written death threat Other (unspecified) threats	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
10	Threaten to release personal information Verbal or written death threat	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				

Below is a list of stalking action pairs. Each action can be an element of a stalking/cyberstalking case. Using the check box, please identify which action is more severe, ***from the perspective of the victim and/or criminal justice system***. Then, using the rating scale, specify the difference in severity between the two cases by circling a number. Circle "1" if both are equal in your mind.

Definitions for Stalking Activity Categories

Courtship behaviors	Engaging target as a stranger in unsolicited conversation in a public place; Offering to by a drink in a public place as a stranger.
Overbearing or Obscene Actions	Making obscene comments as a stranger; Asking for a date more than once after being refused.
Impersonation	Using the victims identity to make obnoxious or worse statements about others; Making offers on the victim's behalf.
Hacking, Trojans, spyware, etc.	Misuse of computer networks to steal information, spy on the victim's actions, or damage victims computer.
Hyperintimacy	Excessive courtship behaviors; Excessive communications attempts; many unwanted gifts.
Pursuit, Proximity, & Surveillance	Lying in wait; Synchronizing activities; Unauthorized photos; Following; Drive-bys.
Invasion, Theft, Vandalism	Property invasion; Information theft; Property theft or damage.
Proxy Pursuit & Intrusion	Involve 3rd Parties for information gathering or proximity opportunities; Intimidate via intermediaries.
Intimidation, Slander, & False Charges	Includes Sabotage and Reputational Harassment. Blackmail; Threats of disclosure to employer; Making false claims to CPS.
Coercion & Constraint	Extortion; Use of physical force; Kidnapping.
Aggression	Assault on property, pets, self, or others; Violence towards victim; Rape; Endangerment;

	Stalking Action Pairs	More Severe	Equally Severe	Somewhat More Severe	Significantly More Severe	Substantially More Severe	Extremely More Severe
1	Obnoxious or Obscene Actions Courtship behaviors	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
2	Hacking, Trojans, spyware, etc. Impersonation	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
3	Impersonation Obnoxious or Obscene Actions	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
4	Hyperintimacy Hacking, Trojans, spyware, etc.	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
5	Invasion, Theft, Vandalism Pursuit, Proximity, & Surveillance	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
6	Intimidation, Slander, & False Charges Proxy Pursuit & Intrusion	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
7	Pursuit, Proximity, & Surveillance Hyperintimacy	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
8	Coercion & Constraint Intimidation, Slander, & False Charges	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
9	Proxy Pursuit & Intrusion Invasion, Theft, Vandalism	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
10	Aggression Coercion & Constraint	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				
11	Courtship behaviors Hacking, Trojans, spyware, etc.	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9				

12	Impersonation Pursuit, Proximity, & Surveillance	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9
13	Hacking, Trojans, spyware, etc. Invasion, Theft, Vandalism	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9
14	Obnoxious or Obscene Actions Hyperintimacy	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9
15	Invasion, Theft, Vandalism Coercion & Constraint	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9
16	Hyperintimacy Proxy Pursuit & Intrusion	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9
17	Proxy Pursuit & Intrusion Aggression	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9
18	Pursuit, Proximity, & Surveillance Intimidation, Slander, & False Charges	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9
19	Proxy Pursuit & Intrusion Courtship behaviors	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9
20	Coercion & Constraint Impersonation	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9
21	Intimidation, Slander, & False Charges Obnoxious or Obscene Actions	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9
22	Aggression Hacking, Trojans, spyware, etc.	☐ ☐	1 — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9

Demographic Information

This information will be used to characterize your expertise in our reports on this research. No personally identifiable information will be used or publicly disclosed. Location specific information will not be used (e.g. city names).

What is your job title? _____

What organization do you work for? _____

How long have you been working with victims or in the criminal justice system? _____

Briefly describe your experience with stalking or harassment cases or victims:

APPENDIX D:

INSTITUTIONAL REVIEW BOARD APPROVAL LETTER

Oklahoma State University Institutional Review Board

Date:	Thursday, July 20, 2006
IRB Application No	BU0631
Proposal Title:	Cyberstalking Severity: A Study of Incident Severity Using Archival Data
Reviewed and Processed as:	Exempt

Status Recommended by Reviewer(s): Approved Protocol Expires: 7/19/2007

Principal Investigator(s

Stephen D. Barnes
3501 W. 24th Ave.
Stillwater, OK 74074

Rick Wilson
408 Business
Stillwater, OK 74078

The IRB application referenced above has been approved. It is the judgment of the reviewers that the rights and welfare of individuals who may be asked to participate in this study will be respected, and that the research will be conducted in a manner consistent with the IRB requirements as outlined in section 45 CFR 46.

☑ The final versions of any printed recruitment, consent and assent documents bearing the IRB approval stamp are attached to this letter. These are the versions that must be used during the study.

As Principal Investigator, it is your responsibility to do the following:

1. Conduct this study exactly as it has been approved. Any modifications to the research protocol must be submitted with the appropriate signatures for IRB approval.
2. Submit a request for continuation if the study extends beyond the approval period of one calendar year. This continuation must receive IRB review and approval before the research can continue.
3. Report any adverse events to the IRB Chair promptly. Adverse events are those which are unanticipated and impact the subjects during the course of this research; and
4. Notify the IRB office in writing when your research project is complete.

Please note that approved protocols are subject to monitoring by the IRB and that the IRB office has the authority to inspect research records associated with this protocol at any time. If you have questions about the IRB procedures or need any assistance from the Board, please contact Beth McTernan in 415 Whitehurst (phone: 405-744-5700, beth.mcternan@okstate.edu).

Sincerely,

Sue C. Jacobs, Chair
Institutional Review Board

CONSENT TO PARTICIPATE IN A RESEARCH STUDY
OKLAHOMA STATE UNIVERSITY

PROJECT TITLE: Cyberstalking Activity Severity Comparison

INVESTIGATORS: Stephen Barnes, Doctoral Candidate, MS, Management Science and Information Systems Department, Spears School of Business, Oklahoma State University

Research Advisors: Dr. David Biros, Assistant Professor, and Dr. Rick Wilson, Dept. Chair, Management Science and Information Systems Department, Spears School of Business, OSU.

PURPOSE:

Cyberstalking is stalking perpetrated exclusively or largely with computer mediated communications and/or other online applications and services. In other words, using the Internet. This research project is attempting to analyze records of historical cases of cyberstalking and online harassment to understand the forms that cyberstalking takes, and how the Internet has affected traditional stalking.

To achieve our research goals, we need to characterize online actions that can be a part of cyberstalking as well as traditional stalking. A critical component of this is to understand the relative levels of severity represented by each stalking action type in comparison with other stalking actions. This survey will be used to measure the perceived differences in severity for paired stalking actions and threats. The resulting data will be mathematically combined with the historical data to develop a severity score for each case. That case severity score will then be used in combination with other information to inform our broader research into cyberstalking.

PARTICIPANTS

You have been invited to participate as an professional involved with the processes that support victims of stalking, or are involved in a related area of the criminal justice system.

PROCEDURES:

The project will involve completion of one questionnaire. This questionnaire consists of a list of pairs of cyberstalking activities, and asks you to indicate the relative differences in severity between the activities in the pair.

The study is designed to last approximately 30-60 minutes.

RISKS OF PARTICIPATION:

There are no risks associated with this project, including stress, psychological, social, physical, or legal risk which are greater, considering probability and magnitude, than those ordinarily encountered in daily life. If, however, you begin to experience discomfort or stress in this project, you may end your participation at any time.

BENEFITS OF PARTICIPATION:

You may gain an appreciation and understanding of how research is conducted.

CONFIDENTIALITY:

All information about you will be kept confidential and will not be released. Questionnaires and record forms will have identification numbers, rather than names, on them. All information will

be kept in a file cabinet that is accessible only to the researchers and their assistants. This information will be saved as long as it is scientifically useful; typically, such information is kept for five years after publication of the results. Results from this study may be presented at professional meetings or in publications. You will not be identified individually; we will be looking at the group as a whole.

Confidentiality will be maintained except under specified conditions required by law. For example, current Oklahoma law requires that any ongoing child abuse (including sexual abuse, physical abuse, and neglect) of a minor must be reported to state officials. In addition, if an individual reports that he/she intends to harm him/herself or others, legal and professional standards require that the individual must be kept from harm, even if confidentiality must be broken. Finally, confidentiality could be broken if materials from this study were subpoenaed by a court of law.

COMPENSATION:

There is no compensation for participation in this activity. We do however thank you for your willingness to contribute to this research and the advancement of science generally.

CONTACTS:

I understand that I may contact any of the researchers at the following addresses and phone numbers, should I desire to discuss my participation in the study and/or request information about the results of the study: Stephen D. Barnes, M.S., Spears School of Business, Dept. of Management Science and Information Systems, Oklahoma State University, Stillwater, OK 74078, (405) 744-4078, or at stephen.barnes@okstate.edu. I may also contact Sue Jacobs, Ph.D., Institutional Review Board, 415 Whitehurst, Oklahoma State University, Stillwater, OK 74078, (405) 744-1676 with any questions concerning participant's rights.

PARTICIPANT RIGHTS:

I understand that my participation is voluntary, that there is no penalty for refusal to participate, and that I am free to withdraw my consent and participation in this project at any time, without penalty.

CONSENT DOCUMENTATION:

I have been fully informed about the procedures listed here. I am aware of what I will be asked to do and the benefits of my participation. I also understand the following statements:

I affirm that I am 18 years of age or older.

I have read and fully understand this consent form. I sign it freely and voluntarily. A copy of this form will be given to me. I hereby give permission for my participation in the study.

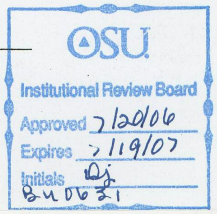
_____ _____

Signature of Participant Date

I certify that I have personally explained this document before requesting that the participant sign it.

_____ _____

Signature of Researcher Date



VITA

Stephen Dean Barnes

Candidate for the Degree of

Doctor of Philosophy

Thesis: THE IMPACT OF COMPUTER MEDIATED COMMUNICATIONS ON STALKING SEVERITY: AN EXPLORATORY ANALYSIS OF CYBERSTALKING FIELD DATA

Major Field: Management Science and Information Systems

Biographical:

Education: Received Bachelor of Arts in Linguistics from the University of Washington, Seattle, Washington in June 1983. Completed the requirements for the Masters of Science with a major in Telecommunications at the University of Colorado, Boulder, Colorado, in May 1991. Completed the Requirements for the Doctor of Philosophy degree in Business Administration at Oklahoma State University, Stillwater, Oklahoma, in December 2007.

Experience: Professional Research Assistant, University of Colorado, 1983-96.
International Partner, Habitat for Humanity, 1986-88.
Graduate Teaching Assistant, University of Colorado, 1989-91.
Research Assistant, Cable Laboratories, 1991.
Contract Software Designers, AGS Information Services, 1991.
Engineer, Consultant, Manager, Nortel Networks, 1991-2001.
Graduate Teaching Assistant, Oklahoma State University, 2002-07.

Professional Memberships: Institute for Electrical and Electronic Engineers, Association for Information Systems.

Name: Stephen Dean Barnes Date of Degree: December, 2007

Institution: Oklahoma State University Location: OKC or Stillwater, Oklahoma

Title of Study: THE IMPACT OF COMPUTER MEDIATED COMMUNICATIONS ON STALKING SEVERITY: AN EXPLORATORY ANALYSIS OF CYBERSTALKING FIELD DATA

Pages in Study: 117 Candidate for the Degree of Doctor of Philosophy

Major Field: Management Science and Information Systems

Scope and Method of Study: The interaction between disjunctive interpersonal relationships, those where the parties disagree on the goals of the relationship, and the use of computer mediated communications (CMC) channels is a relatively unexplored domain. Bargh (2002) suggests that use of CMC channels can amplify the development of interpersonal relationships, and notes that the effect is not constant across communication activities. This dissertation reports on a line of research that explores the interaction between CMC and stalking, a common form of disjunctive relationship. CMC channels can be characterized by their richness, interactivity, and distribution (Te'eni 2001). Field data from cyberstalking cases is used to examine the effects of CMC channels on stalking case severity, and to explore the relative impacts of CMC channel characteristics on such cases.

Findings and Conclusions: To accomplish this, a ratio-scaled measure of stalking case severity is developed for exploring the relationship between case severity and CMC media characteristics. This includes levels of anonymity, as well as the prior relationship between the stalker and the victim. Results show that channel richness and the nature of the prior relationship dominate the impact on cyberstalking case severity, while channel interactivity, distribution, and harasser anonymity do not affect case severity. In conclusion, this analysis of cyberstalking data provides support for Te'eni's (2001) CAMOC model and its interpretation of media richness theory. Further, the analysis provides evidence that disjunctive online relationships are different from disjunctive offline relationships only when intimacy is involved. Follow-up research is proposed along with suggestions for the development of an improved measure of case severity.

ADVISER'S APPROVAL: Rick L. Wilson