Article

Journal of Interpersonal Violence
2017, Vol. 32(10) 1451–1475

DOI: 10.1177/0886260515589564
journals.sagepub.com/home/jiv
SAGE

Cyber-Defense: A Taxonomy of Tactics for Managing Cyberstalking

Robert S. Tokunaga[1] and Krystyna S. Aune[1]

Abstract

Cyberstalking research has revealed information about who is perpetrating what offense to whom. This study adds to research on cyberstalking by exploring how victims respond to the unwanted pursuit. The reflections of cyberstalking victims were content analyzed to answer research questions about different risk management behaviors, their effectiveness, and their relationship with specific cyberstalking behaviors. Findings indicated that victims used seven general management tactics of which ignore/avoidance, active technological disassociation, and help seeking were the most common. Using technology to move away from pursuers was reported as the most effective tactic for managing the unwanted relational pursuit. The results also suggested that victims' management responses were associated with the type of behaviors experienced.

Keywords

cyberstalking, victimization, risk management, tactics, thematic analysis, Internet

The threat of cyberstalking victimization and other forms of online unwanted relational pursuit are existential concerns for Internet users. Internet technologies, given their favorable affordances, can create hospitable environments for these

[1]University of Hawai'i at Mānoa, Honolulu, HI, USA

Corresponding Author:
Robert S. Tokunaga, Department of Communicology, University of Hawai'i at Mānoa, George Hall 326, 2560 Campus Rd., Honolulu, HI 96822, USA.
Email: robert.tokunaga@hawaii.edu

deviant behaviors (Suler, 2004). Online affordances that encourage deviant behaviors include anonymity, asynchronicity, and the absence of a policing agent (Bubas, 2001). Cyberstalking is also not inhibited by barriers such as geographical distance and scheduling (Holt & Bossler, 2009; Reyns, Henson, & Fisher, 2012). Numerous cases of cyberstalking are reported each year, signaling the importance of studying this phenomenon. Prevalence estimates suggest that about 20% to 40% of Internet users are victimized by a cyberstalker (Baum, Catalano, Rand, & Rose, 2009; D'Ovidio & Doyle, 2003; Fisher, Cullen, & Turner, 2000; Jerin & Dolinsky, 2001; Reyns et al., 2012; Spitzberg & Hoobler, 2002).

Cyberstalking can have profound negative psychological and behavioral effects on victims (Parsons-Pollard & Moriarty, 2009). Victims often undergo persistent psychological impairment, such as depression, and wrestle with issues of personal insecurity (Dreßing, Bailer, Anders, Wagner, & Gallas, 2014; Nobles, Reyns, Fox, & Fisher, 2014; Pathé & Mullen, 1997). The psychological distress that victims of cyberstalking exhibit is similar in nature to what is experienced by traditional stalking victims (Glancy, Newman, Potash, & Tennison, 2007). Behavioral problems that arise from cyberstalking include increased sleeplessness, social withdrawal, and changes to regular social habits (Dreßing et al., 2014). Although empirical interest in the prevalence and negative effects of cyberstalking is growing (Bocij, Griffiths, & McFarlane, 2002; Melander, 2010), systematic research in the area of risk management behaviors to counter cyberstalking is noticeably sparse. Nobles et al. (2014) recognized that cyberstalking research "has not developed to the point where patterns in responses to victimization, including self-protective behaviors taken by the victim, have been clearly identified" (p. 8). A comprehensive taxonomy (i.e., a systematic classification) of offline stalking management strategies took long to develop because the nature of the deviant behavior is fraught with complexity and its endemic criminalization occurred only recently (Storey & Hart, 2011). For these same reasons, a well-developed taxonomy of behaviors used to manage the risks involved with cyberstalking has not been constructed.

The rare attempts to identify various approaches to managing risks of cyberstalking in existing research have been unsystematic. In other words, the content selected in these taxonomies has relied on those who constructed them. The aim of this exploratory investigation is to develop a comprehensive taxonomy of risk management tactics used by cyberstalking victims through a thematic analysis of their written reflections. This analysis involves the identification of themes of common management tactics that emerge out of victims' responses without preconceptions about this set of behaviors. The term *victim* is used to reference targets of cyberstalking perpetration, with the

qualification that some of these individuals do not see themselves as victims (see Karmen, 2012). Creating a taxonomy of management tactics for cyberstalking is an important research pursuit because it could point to concrete behaviors future victims can use to manage these encounters. This taxonomy is also important in light of the growing number of cases of cyberstalking perpetration. A newtaxonomy would be helpful to counselors, practitioners, the legal community, and social scientists who study the "dark side" of Internet use. The second goalis to distinguish management tactics that have been effective from ineffective ones. Finally, the third goal is to examine the relationship between cyberstalking behaviors and these management tactics to determine the suitability of victims' responses for managing the risks of specific cyberstalking events, which can range considerably in their form, function, and severity.

Relational Intrusions Native to Technology Use

Cyberstalking is the repeated unwanted relational pursuit of an individual through communication technologies, such as computers, tablets, and smart phones (Goodno, 2007; Reyns et al., 2012). Internet technologies are enticing platforms for stalkers because they create unique opportunities for perpetration (Nobles et al., 2014; Reyns, Henson, & Fisher, 2011). Although many types of cyberstalking have been documented, behaviors involving the pursuit of unwanted relationships using technologies are of main interest to those who study interpersonal violence. McFarlane and Bocij (2003) used the term *intimate cyberstalkers* to describe the group of individuals, which includes ex-intimates and infatuates, who use technology for unwanted relational pursuit. Intimate cyberstalking can involve psychological intimidation and threats made between people in existing relationships, but individuals not involved in a relationship can also be pursued (Southworth, Finn, Dawson, Fraser, & Tucker, 2007).

Confusion surrounds the term *cyberstalking* because it is used aside colloquial phrases such as Facebook stalking or friend stalking. In public discourse, Facebook or friend stalking refers to surreptitious online information-seeking behaviors (Lyndon, Bonds-Raacke, & Cratty, 2011; Parsons-Pollard & Moriarty, 2009; Tokunaga, 2011, 2016), whereas cyberstalking involves the repeated pursuit of a targeted individual over the Internet (Reyns et al., 2011). Cyberstalking is sometimes viewed as an analog to offline stalking but enacted through the Internet (Tjaden, 2014). To determine what tactics individuals use to manage the risks of cyberstalking victimization, information about the behaviors they are responding to must be reviewed.

Dimensions of Cyberstalking Behaviors

Cyberstalking is often viewed as an extension of offline stalking given their conceptual and operational overlap. With this said, a set of stalking behaviors specific to the Internet domain has been cataloged in prior research. Spitzberg and Hoobler's (2002) taxonomy explicated the various behaviors perpetrated by cyberstalkers. The taxonomy was created through an extensive literature review of law, psychology, and popular press publications in addition to a qualitative examination of open-ended responses in pilot studies. The classification system, which includes hyperintimacy, threat, sabotage, and invasion behaviors, is organized by severity and threat. Hyperintimacy reflects the most commonly reported and least threatening types of cyberstalking behaviors, whereas invasion is the least common but often most menacing form of cyberstalking.

Hyperintimacy. Hyperintimacy involves messages delivered electronically or digitally in relentless pursuit of a relationship. Hyperintimate messages are generally harmless but nonetheless considered harassment (LeBlanc, Levesque, Richardson, & Berka, 2001; Spitzberg & Hoobler, 2002). Hyperintimacy online can be communicated as affection expression, ingratiation, relational repair, or hypersexuality (Cupach & Spitzberg, 2000). In affection expression, pursuers repeatedly communicate messages about a desired relationship despite several attempts by the victim to rebuff the requests. Ingratiation involves pursuers sending unsolicited messages of assistance, compliments, and positive regard to victims. Relational repair includes messages that communicate a preferred relational state. Finally, pursuers sometimes send text-based messages or images that include graphic nonviolent sexual content called hypersexual messages. Hyperintimate messages sent through email, instant messenger, or other Internet platforms most often include tokens of affection, demands for a relationship, and excessive personal disclosures.

Threat. Threat messages in online relational pursuit involve implicit or explicit claims of harm to the target (Spitzberg & Hoobler, 2002). Threats of harm can range in form from harming one's reputation to more sinister acts of bodily injury. Victims' reputations or public images can be threatened with the dissemination of real or falsified information. Their public face is often threatened in their private lives, at their workplaces, or at school. Threats can also include vague statements implying that "something bad" is going to happen to the victim or suggesting specific harm to one's property, economic livelihood, family, or friends. In the most extreme cases, threats of physical harm or even death are communicated online.

Sabotage. Sabotage is executed when victims' reputations are compromised by either true or fabricated information (Spitzberg & Hoobler, 2002). One's personal character is assaulted by spreading rumors or gossip to others close to the victim (Wolke, Woods, Bloomfield, & Karstadt, 2000). Cyberstalkers often sabotage the public image of victims in their social or professional lives. A cyberstalker can socially sabotage victims' reputations by sending unattractive or embarrassing messages about them to their friends, families, or current romantic partners (Spitzberg & Hoobler, 2002). Professional sabotage involves the propagation of character attacks in the victims' organization or school.

Invasion. Invasion is considered the most menacing set of cyberstalking behaviors because it involves actions that profoundly interfere with victims' livelihoods. These behaviors can extend to property damage and identity theft (Spitzberg & Hoobler, 2002). Information theft and exotic surveillance are two main types of invasion behaviors. Cyberstalkers sometimes attempt to and succeed in gathering private information about their victims over a communication technology (Bocij, 2004). The most common way this information is collected is by hacking into victims' computers or the computers of close others. In an effort to collect information, pursuers can also assume the identity of their victims and impersonate them in online correspondence to family and friends (McFarlane & Bocij, 2003). Exotic surveillance occurs when pursuers actively monitor the victims' whereabouts by bugging computers or mobile technologies (Pathé & Mullen, 1997). Exotic surveillance is most commonly performed through global positioning system (GPS) tracking programs and key logging devices that record and send back to pursuers everything victims type on their computers. These devices are surreptitiously installed on victims' smart phones or computers without their knowledge. Because invasion behaviors require a set of skills possessed only by those with considerable computer and Internet expertise, invasion is the least commonly encountered form of cyberstalking.

Offline and Online Stalking

Cyberstalking is conceptualized as an "extension of stalking that utilizes computers and other electronic devices or as a completely separate action that has some of the elements of stalking but utilizes a different mode of delivery" (Parsons-Pollard & Moriarty, 2009, p. 435). This definition underscores two discrepant perspectives about the nature of cyberstalking in the literature: one that sees cyberstalking as a mere extension of offline stalking and the other that views cyberstalking as a behavior with unique

characteristics (Alexy, Burgess, Baker, & Smoyak, 2005; Bocij & McFarlane, 2002; Nobles et al., 2014; Parsons-Pollard & Moriarty, 2009; Spitzberg & Hoobler, 2002; Wall, 2005). Those who argue for the extension perspective point to evidence that demonstrates the considerable overlap between cyberstalking and offline stalking. Prevalence estimates of cyberstalking are comparable with offline stalking when equivalent criteria are used to identify genuine cases (Dreßing, Bailer, Anders, Wagner, & Gallas, 2014). Sheridan and Grant (2007) found that the process of cyberstalking, its effects on victims and other third parties, and response strategies are also indistinguishable from offline stalking.

The nature of the stalking may differ between the offline and online domains to the extent that the relationship between the pursuer and victim (Sheridan & Grant, 2007), pursuers' demography (Strawhun, Adams, & Huss, 2013), and pursuers' criminal history (Baker, 1999; Lucks, 2004) change as a function of the medium through which the stalking is undertaken. These differences between offline and online stalking indicate that the communication medium plays a central role in the process (Melander, 2010; Reyns, 2010; Reyns et al., 2012). In cyberstalking, only a modest proportion of victims know the identity of the perpetrator; these perpetrators often concealed their identity through the Internet (Finkelhor, Mitchell, & Wolak, 2000). Known perpetrators who were prosecuted in the criminal justice system rarely have a prior criminal history unlike offline stalkers (Lucks, 2004). The absence of criminal histories may be an indication that the disinhibitive potential of some communication technologies encourages antisocial behaviors that would otherwise be self-regulated offline. It is possible that online anonymity creates new opportunities for pursuers to take greater risks in perpetrating deviant behaviors (Glancy et al., 2007). Melander's (2010) qualitative analysis of online relational pursuit among college students uncovered several behaviors uniquely tied to Internet use. Pursuing a relationship from afar through a technology often tethered to the victim makes cyberstalking perpetration convenient and enticing for some.

The Present Study

Victims of hyperintimacy, threat, sabotage, and invasion behaviors manage risks using a variety of tactics. Management tactics refer to specific behaviors enlisted by victims to end or mitigate future online pursuit (Storey & Hart, 2011). Taxonomies of behaviors to manage offline stalking and other forms of obsessive relational intrusion used by victims (Cupach & Spitzberg, 2004; Spitzberg, Nicastro, & Cousins, 1998) and police (Storey & Hart, 2011) have

been previously created. No prior study, however, has attempted to systematically create a taxonomy of risk management tactics for cyberstalking. Such a taxonomy will identify areas of overlap with behaviors enacted by victims of offline stalking, but the analysis may also uncover risk management tactics unique to the online domain. In this study, three research questions are proposed to explore a taxonomy of cyberstalking management behaviors and distinguish effective from ineffective tactics in response to specific cyberstalking behaviors.

Many management tactics are common to offline and online stalking victimization, but there may be reason to believe that nuanced responses to cyberstalking exist as well. Victims of offline and online stalking used similar management behaviors, such as help seeking, ignoring the pursuit, and confronting the stalker (Sheridan & Grant, 2007). However, in examining responses to relational stalking over the telephone, Spitzberg et al. (1998) found management tactics specific to the medium through which stalking occurred. Victims used inexpensive and easily accessible technologies, such as caller ID and call-back capabilities on telephones, to manage the pursuit (Spitzberg & Cupach, 1996). Nobles et al. (2014) argued that "compared to stalking, it is possible that the nature of cyberstalking elicits a very personal violation for victims, which may elicit more diverse and more frequent protective actions" (pp. 21-22). Ataxonomy of management behaviors can uncover the diverse protective actions cyberstalking victims use that are similar and different to those used by victims of offline stalking.

Research Question 1: What tactics do victims of cyberstalking recall in managing their encounters?

The objective of this formative investigation is to reach a comprehensive understanding of the types of management tactics that victims use in cyberstalking situations, but applied implications should also be considered. Ascertaining the efficacy of these tactics during and after victimization would support the practical applications of this study by helping clinicians, legal professionals, counselors, and others develop better intervention strategies. Distinguishing effective from ineffective management tactics would also directly benefit cyberstalking victims, providing them with direction about steps they can take to manage the risks associated with these deviant behaviors.

Research Question 2: What management tactics do cyberstalking victims report as effective in ending the pursuit or preventing future pursuit?

Information about the effectiveness of management tactics presents an incomplete picture of how victims manage the risks associated with cyberstalking. A second important component of risk management is examining the relationship between cyberstalking behaviors and their attendant management tactics. An examination of this association uncovers information about the behavioral responses most often used to manage a given set of cyberstalking behaviors. The absence of a relationship implies that the management tactics are uniformly distributed across the four types of cyberstalking behaviors. A significant association, alternatively, would indicate that victims mindfully apply specific management tactics to address certain cyberstalking behaviors. Also, because cyberstalking behaviors are arranged by frequency and severity, an examination of this relationship may provide an organization to the taxonomy constructed in this investigation by indicating the tactics most appropriate to and effective for a cyberstalking episode ranging in degrees of severity.

Research Question 3: Is there a relationship between cyberstalking behaviors and risk management tactics?

Method

Procedure

Two recruitment methods were used in this study. Undergraduate students at a large U.S. university were recruited through communication courses. Students were given information about the study and invited to participate if they met the study requirements. Students could only complete the questionnaire if they had encountered an event where another person, either a stranger or known other, repeatedly pursued an unwanted relationship online. Because the college student sample was not representative of the larger population of Internet users, and likely experienced only a limited subset of cyberstalking behaviors, an Internet sample was also recruited. Recruitment letters were placed on two popular support websites for victims of cyberstalking: CyberAngels and Women Halting Online Abuse (WHOA). Visitors of these websites were informed about the study and invited to participate if they had encountered cyberstalking.

Victimization is a sensitive discussion topic that may elicit anxiety and concentration impairments in the presence of an interviewer (Brzuzy, Ault, & Segal, 1997). Inquiring about behaviors victims undertook in response to cyberstalking during an in-person interview could also increase the likelihood

of socially desirable response biases. To minimize bias in the reflections, a survey design was used. The survey design allows participants to complete a questionnaire anonymously at their leisure in a safe and anonymous environment. The college student sample completed a paper-and-pencil form of the open-ended questionnaire, whereas the Internet sample completed an identical questionnaire through an Internet-based service (i.e., Survey Share). Students were given research credit for their participation, whereas the Internet sample was not incentivized.

Participants

A total of 51 victims of cyberstalking (14 males, 37 females) completed the questionnaire. The sample included 43 students and 8 Internet participants. The sample was large enough to reach saturation, as evidence by the same responses mentioned reliably by several independent respondents. The frequencies of each reported instance of a management tactic in the results provide a quantitative estimate of this achieved saturation point. The average age of the sample was 23.35 years ($SD = 6.73$, range = 18-48 years). The ethnicities of the sample were reported as follows: 45.1% ($n = 23$) Asian, 31.4% ($n = 16$) Caucasian, 15.7% ($n = 8$) mixed, 3.9% ($n = 2$) Hawaiian/Pacific Islander, 2.0% ($n = 1$) Native American, 2.0% ($n = 1$) African American/African.

A majority of the participants (70.6%, $n = 36$) were pursued by males, and the median length of time of the overall pursuit was 30 days ($M = 189.69$, $SD = 345.91$). The median number of times a pursuer made contact with the participant was 9 times a month ($M = 15.27$, $SD = 19.11$). The type of relationship that participants had with their pursuers prior to the cyberstalking behaviors was reported as follows: 47.0% ($n = 24$) stranger, 19.6% ($n = 10$) acquaintanceship, 13.7% ($n = 7$) friendship, 7.8% ($n = 4$) serious dating relationship, 2.0% ($n = 1$) colleague or service relationship, 2.0% ($n = 1$) casual dating relationship, 2.0% ($n = 1$) ex-spouse, and 5.9% ($n = 3$) other. The median length of the relationship was approximately 25 days ($M = 74.35$, $SD = 125.58$) before becoming unwanted. Lastly, participants reflected on experiences that occurred approximately 1 year ago ($M = 1.63$ years ago, $SD = 1.92$, range = currently ongoing to 9 years).

Instrument

Cyber-Obsessional Pursuit Scale (COP). A 19-item scale by Spitzberg and Hoobler (2002) was used to assess the frequency of participants' encounters with specific cyberstalking behaviors. The COP includes four subscales, with

items that contain examples of hyperintimacy (e.g., sending exaggerated messages of affection), threat (e.g., directing others to you in threatening ways), sabotage (e.g., sabotaged your private reputation), and invasion (e.g., obtaining private information without permission) behaviors. Participants were asked how many times they had encountered a specific cyberstalking behavior. The anchors of the scale to measure frequency were situated at 0 (*no experience*) and 4 (*over 5 times*).

Managing cyberstalking. Open-ended questions were positioned after each cyberstalking behavior of the COP to describe the action(s) that respondents took to manage it. The instructions stated, "In the space provided here, please describe in detail any action(s) you took in response to this behavior." Participants were given six lines of text to respond to the open-ended question, "What specific actions did you take to end this behavior or prevent this behavior from happening in the future?"

Response effectiveness. After each open-ended response, a one-item statement asked participants to rate the effectiveness of the response in stopping the cyberstalking behavior. Participants were asked to rate on a 7-point Likert-type scale their agreement with the statement "I felt that the response listed above was effective in stopping the behavior." The anchors of the response effectiveness scale were 1 (*not at all successful*) and 7 (*extremely successful*). Higher values indicate that the response was effective in managing the cyberstalking behavior.

Results

Analysis

A thematic content analysis was undertaken to code responses from the open-ended questions. Independent tactics for each cyberstalking behavior, not individual respondents, were treated as the unit of analysis. The open-ended questionnaire generated 268 interpretable management tactics to the 19 cyberstalking behaviors among the 51 victims of cyberstalking. The initial thematic coding analysis conducted on the 19 items yielded a list of 28 independent tactics (see Table 1). Similar tactics were condensed through a subsequent analysis, resulting in a smaller set of seven management tactics, to achieve greater parsimony. A quantitative coding analysis was conducted subsequent to the thematic analysis by two undergraduate students, using a coding scheme prepared by the investigator, to answer the research questions. The metric for intercoder reliability indicated acceptable agreement between the coders (Scott's $\pi = .86$).

Table 1. Initial Thematic Coding of Management Tactics to the Cyberstalking.

Tactics
Strategy 1: Ignore/avoidance
1. Ignore
2. Avoided sites and programs that pursuer contacted him or her through
3. Changed the subject
4. Deleted messages before reading them
5. Acted like it did not bother him or her
Strategy 2: Active technological disassociation
6. Deleted old account and made a new account
7. Deleted/declined pursuer as a friend
8. Made information private so that only accepted "friends" could access it
9. Blocked pursuer's messages
Strategy 3: Help seeking
10. Contacted local law authorities/filed charges
11. Kept a hardcopy of all written evidence
12. Hired a team of private investigators
13. Asked a third party to respond to the pursuer
14. Got help through a support website
15. Reported the pursuer to the web owner/Internet Service Provider (ISP)
Strategy 4: Negotiation/threat
16. Threatened the pursuer
17. Argued with the pursuer
18. Told the pursuer that he or she wanted it to stop/was not interested
Strategy 5: Compliance/excuses
19. Played along
20. Falsely disclosed about themselves
21. Made excuses of not being able to or wanting a relationship
Strategy 6: Technological privacy maintenance
22. Changed profile picture
23. Changed username and/or password
24. Changed email addresses
25. Downloaded antivirus software
Strategy 7: Derogation
26. Confronted the pursuer as a fraud
27. Directly insulted the pursuer
28. Posted a public discursive note to the pursuer

Risk Management Tactics

The first research question explored the constellation of tactics victims of cyberstalking used to manage the relational pursuit. Victims were asked what

behaviors they enacted to end the cyberstalking encounters or prevent future ones from happening. The content analysis produced a list of seven unique management tactics, which were organized by the frequencies in which they were used. The management tactics are ignore/avoidance, active technological disassociation, help seeking, negotiation/threat, compliance/excuses, technological privacy management, and derogation. Each of these management tactics will be discussed in the following subsections.

Ignore/avoidance. A content analysis of the responses indicated that the most commonly used management tactic was to ignore or avoid the cyberstalking encounter (n = 96, 35.82%). Most victims used this tactic because they believed that ignoring the behaviors would help to mitigate the pursuit. In a reflection representative of victims in the sample, a female respondent explained her reasons for using the ignoring/avoidance tactic after receiving online messages that suggested direct or indirect harm to her, her family members, or her property:

> I did nothing. I didn't know what to do and I did nothing, hoping if I ignored it, it would go away. (Female, 35 years old)

Active technological disassociation. The second most common management tactic involved victims who use certain functions of the technology to end and prevent future cyberstalking encounters. The factor, labeled *active technological disassociation*, was used 20.15% (n = 54) of the time. Victims provided numerous examples of how they disassociated themselves from the cyberstalking pursuit that included making online information private to only verifiable "friends" and blocking the pursuer from contacting them through the features available in the technology. In response to receiving exaggerated messages of affection online, a victim recalled how she blocked the pursuer through the technology's settings:

> I did nothing much. I put him under the spam-mail and blocked his Internet Protocol (IP) address in the chat room. (Female, 24 years old)

A second respondent also reported his use of certain features of the instant messenger, ICQ, to block messages from an unknown pursuer.

> E.L. requested to join my ICQ list. I was curious as I was new to the ICQ program and just accepted E.L. into my safe list. Then nasty stuff came out. E.L. not only used ICQ to talk about adulterous topics but also sent emails to me as well. I had to block E.L. from my safe list of ICQ. (Male, 36 years old)

Help seeking. Obtaining help from an outside source was cited as a popular way to end cyberstalking behaviors and/or prevent future pursuit from recurring. Most victims who executed this strategy, called *help seeking*, reported filing criminal charges with local law enforcement, reporting the intrusion to website hosts or Internet Service Providers (ISPs), or accessing information and/or guidance from online support websites. A few victims reported taking more proactive measures, such as keeping a hardcopy of all evidence, using a third-party member to bully the pursuer, or even hiring a team of private investigators to manage cyberstalking. The help-seeking strategy was used 18.28% (n = 49) of the time. A female described how she sought help from multiple sources when she encountered a stranger pretending to be someone he or she was not online:

> I hired a private investigation team to handle the issues and deal with the District Attorney to have charges filed. I hired a PI team as nothing else worked. I also worked with Women Halting Online Abuse (WHOA), an organization created to help people being abused online, as well as contacting CyberAngels. (Female, 43 years old)

Negotiation/threat. The *negotiation/threat* tactic, marked by discursive and direct confrontation with pursuers, was used 13.81% (n = 37) of the time. Specific behaviors used to manage the risks associated with cyberstalking included direct interactions threatening legal action or bodily harm, arguing with the pursuer, and telling the pursuer to stop or that there was no interest in a relationship. Many victims discursively "told [the pursuer] to f— off" (Female, 19 years old), but a respondent recalled, in more detail, her experience with managing unwanted tokens and exaggerated messages of affection online using negotiation tactics:

> After adding many of my friends and reading my comments, he was able to find out my AIM screen name, what school I attended, and the activities I did, etc. He messaged me saying he was going to visit my school to see me or show up at my practices. I asked him to stop and that I wasn't interested. I kept telling the person that I don't have the same feelings back and that I didn't care. (Female, 18 years old)

Compliance/excuses. A fifth strategy, labeled *compliance/excuses*, was identified in the collection of victims' reflections. Compliance and excuses were used 6.34% (n = 17) of the time. Victims who used compliance played along with the pursuit, even going so far as to falsely disclose personal information. Victims of cyberstalking also reported making excuses about why they were

unable to enter into a relationship (e.g., currently in a relationship) or why they did not want a relationship at the time (e.g., just got out of a bad relationship). A male victim reflected on his use of compliance to sexually harassing messages from an anonymous stranger online:

> At first, I played along with the other person, thinking it was a friend. I told the other person I was interested in getting to know her better. But the sexual content got more personal and graphic, and I still didn't know who this was. (Male, 19 years old)

Technological privacy management. The specific functions of the technology played a role in a second tactic of managing cyberstalking called *technological privacy management*, which was reported in 2.99% ($n = 8$) of the encounters. This management tactic is signaled by victims who attempt to regain control of their online persona when their privacy was breached. The behaviors used to manage cyberstalking were as innocuous as changing a profile picture on social media to more proactive measures, such as changing email addresses, replacing usernames and/or passwords, or downloading antivirus software to protect personal computers from invasion. A female victim remembered her use of privacy management behaviors in response to someone who assumed her online persona:

> This is related to the people who impersonated me. They email bombed my account, trying to shut it down. I called the ISP and they gave me a new username. (Female, 48 years old)

Derogation. The negotiation/threat tactic introduced the idea that some victims directly confront their pursuers, but another unique tactic involving direct interaction emerged from the analysis. The tactic, labeled *derogation*, was used 2.61% ($n = 7$) of the time. In this risk management behavior, victims confront their pursuers with two goals in mind. For some victims, they confronted the pursuer to insult them. Victims believed that they could manage the pursuit by calling their pursuers "losers," "pathetic," or "cowards." The second reason for confronting pursuers was to call them on their fraudulent behaviors when they pretended online to be someone who they were not. A victim called to mind the steps she took when someone masqueraded as a false persona and sabotaged her private social reputation:

> I told the person directly that I knew this was a fake identity. I kept telling the person I knew what he or she was doing. (Female, 18 years old)

Effectiveness of the Management Tactics

The second research question was aimed at distinguishing the most effective tactics used by victims of cyberstalking from tactics that were less helpful. To accomplish this, the perceived effectiveness ratings for each tactic were reviewed. Technological privacy maintenance, or the action of making information private and available to negotiated contacts, was the most effective strategy in managing the risks associated with the unwanted online pursuit, with a mean of 5.57 ($SD = 2.30$, $n = 8$). Active technological disassociation was the second most successful risk management behavior, with a mean of 4.68 ($SD = 1.73$, $n = 49$). Ignore/avoidance was the third most effective tactic in managing the online pursuit, with an average effectiveness score of 4.16 ($SD = 2.04$, $n = 96$). The ignore/avoidance tactic, aside help seeking, with a mean of 3.96 ($SD = 2.39$, $n = 54$), and negotiation/threat, with a mean score of 3.68 ($SD = 2.25$, $n = 37$), were moderately effective. Compliance/excuses, with a mean score of 2.82 ($SD = 1.47$, $n = 17$), and derogation, with a mean of 2.43 ($SD = 1.81$, $n = 7$), were the least effective methods for managing cyberstalking encounters. These ineffective strategies were used in few instances to manage the threat associated with the cyberstalking events.

Cyberstalking Behaviors and Management Tactics

The relationship between cyberstalking behaviors and management tactics was explored in a 4 (r) × 7 (c) contingency table to address the third research question. The frequencies for each of the seven management tactics were aggregated across the four cyberstalking dimensions (i.e., hyperintimacy, threat, sabotage, and invasion). Table 2 displays the frequencies of encounters with specific cyberstalking behaviors. Fisher's exact test was used to estimate the relationship given that some cells of the contingency table had expected frequencies fewer than five observations. The exact test is appropriate because the sampling distribution of chi-square estimates produces erroneous results when the sample size of the contingency table is small (Upton, 1992). Some, however, argue that Fisher's exact test is too conservative, and its use increases the chances of committing Type II error (Berkson, 1978). Results of the exact test, computed through SPSS 9.4, indicated that cyberstalking behaviors are systematically associated with specific management tactics (Fisher's exact test [two-tailed] = 80.59, $p < .001$), and this association is moderate in magnitude (Cramér's $V = .38$, $p < .001$; see Rea & Parker, 1992 for interpretation of magnitude). The cross-tabulation between cyberstalking behaviors and management tactics is presented in Table 3.

Table 2. Frequencies of Encounters With Cyberstalking Behaviors.

Cyberstalking Behavior	Frequency of Reports	Percent Frequency
Sending tokens of affection	48	94.1
Sending exaggerated messages of affection	37	72.5
Sending excessively disclosive messages	33	64.7
Sending excessively "needy" or demanding messages	32	62.7
Pretending to be someone he or she was not	21	41.2
Sending pornographic/obscene images or messages	17	33.3
Sending sexually harassing messages	15	29.4
Attempting to disable your computer	15	29.4
Exposing private information about you to others	14	27.5
Sabotaging your private or social reputation	14	27.5
Sending threatening written messages	13	25.5
Sabotaging your work/school reputation	8	15.7
Obtaining private information without permission	8	15.7
Using your computer to get information on others	6	11.8
Taking over your electronic identity or persona	6	11.8
Altering your electronic identity or persona	5	9.8
Sending threatening pictures or images	5	9.8
Directing others to you in threatening ways	4	7.8
Bugging your car, home, or office	0	0.0

Note. Out of the 51 respondents, victims who reported at least some experience ("1" or higher) with each specific cyberstalking behavior on the Cyber-Obsessional Pursuit Scale were counted in the frequency.

A closer examination of the observed frequencies in relation to the expected frequencies provides further insight into the association. The ignore/avoidance tactic is used disproportionately in response to hyperintimacy (74.0%) and threat (12.5%) behaviors, but this management behavior became an unattractive choice to victims as the behaviors became more menacing. That is, ignore/avoidance was used to manage sabotage (9.4%) and invasion (4.2%) behaviors in frequencies well below expectation. Frequencies of active technological disassociation and technological privacy management also demonstrated distinguishable patterns across the four cyberstalking behaviors. Active technological disassociation was used in frequencies higher than expected for threat (16.7%), sabotage (31.5%), and invasion (20.4%) behaviors but had lower incidence than expected in managing hyperintimacy (31.5%) behaviors. Moreover, technological privacy management was used exclusively in response to invasion behaviors. The observed count in comparison with the

Table 3. Observed and Expected Frequencies for the Cross-Tabulation of Cyberstalking Behaviors and Management Tactics.

	Ignore/ Avoidance	Active Technological Disassociation	Help Seeking	Negotiation/ Threaten	Compliance/ Excuses	Technological Privacy Maintenance	Derogate	Total
Hyperintimacy								
Observed	71	17	34	25	14	0	1	
Expected	58	32.6	29.6	22.4	10.3	4.8	4.2	162
Threat								
Observed	12	9	3	3	0	0	1	
Expected	10	5.6	5.1	3.9	1.8	0.8	0.7	36
Sabotage								
Observed	9	17	5	7	3	0	5	
Expected	16.5	9.3	8.4	6.1	2.9	1.4	1.2	31
Invasion								
Observed	4	11	7	2	0	8	0	
Expected	11.5	6.4	5.9	4.4	2.0	1.0	0.8	32
Total	96	54	49	37	17	8	7	
Observed percentages (%)	35.8	20.2	18.3	13.8	6.3	3.0	2.6	268

expected frequency suggests that in the minds of victims, active technological disassociation and technological privacy management are appropriate responses for the severer, more menacing, and less common forms of cyberstalking. The observed frequencies of other management tactics did not deviate from their respective expected frequencies in any meaningful pattern.

Discussion

Evolving online lifestyles have ushered in unique challenges for Internet and mobile technology users. The unprecedented access to individuals through communication technologies, which transcends time and geographical limitations, has also created novel opportunities for perpetrating deviant behaviors, such as cyberstalking (Reyns, 2010; Reyns et al., 2011). The intent of this investigation was to understand the range of behaviors victims use to manage unwanted online relational pursuit. The effectiveness of each management tactic and its appropriateness to guard against specific cyberstalking encounters were also examined. The practical utility of this investigation is that practitioners are able to recommend specific actions that have been previously used with some measure of success to manage the risks of specific types of cyberstalking behaviors.

Seven supraordinate risk management behaviors were uncovered in the written reflections of victims who experienced some type of cyberstalking. The redundancy of the responses across victims and situations was one metric for determining that the data reached saturation. The taxonomy systematically derived from the thematic analysis underscored the similarities between offline and online stalking. Some management tactics, however, were unique to the devices used to carry out the unwanted online pursuit. These management tactics unique to the online domain reflect aspects of cyberstalking that are at some level phenomenally distinct from offline stalking.

Similarities in Managing Offline and Online Stalking

The taxonomy revealed several management tactics shared by victims of both offline and online stalking. Victims of cyberstalking directly challenged pursuers by derogating them online. They used profane language or labels such as “pathetic” while communicating with their pursuers. To manage the threat of offline stalking, victims communicate similar types of verbal aggression. Some make angry telephone calls, write irate letters, or initiate in-person confrontations to insult their pursuers (Nicastro, Cousins, & Spitzberg, 2000). Derogating the pursuer, however, was the least helpful tactic for managing the risks associated with cyberstalking. It may be that derogation fueled

anger that, in turn, led to more menacing forms of online pursuit. The direct attacks may have also aroused pursuers, providing them with the social interaction they desired.

Some cyberstalking victims opened communication with their pursuers but in a less hostile manner than those who used online derogation. Victims pleaded with their pursuers to stop and, in some cases, used veiled threats of physical or material harm. Using direct interactions with pursuers to negotiate cessation of the pursuit is also used by victims of offline stalking (Brewster, 2002; Nicastro et al., 2000). Some offline stalking victims pleaded with or cried in front of their pursuers to stop further pursuit. This behavior was moderately effective in ending cyberstalking victimization, but the direct contact between victims and pursuers may have perpetuated the pursuit for some. Clinicians advise victims of offline stalking to alter their lifestyles so as to avoid future interactions with their pursuers (Mullen et al., 2006).

Seeking help from legal authorities was also common for those victimized by cyberstalking. Contacting legal agencies for help is a common solution sought by victims of offline stalking as well (Blaauw, Winkel, & Arensman, 2000; Pathé, Mullen, & Purcell, 2000; Purcell, Pathé, & Mullen, 2000). Cyberstalking victims found that help-seeking behaviors were moderately effective in managing the pursuit, whereas victims of offline stalking often find help seeking unproductive and ineffective. The main criticism made by victims of offline stalking who seek help is that their complaints are met in the legal system with inaction or incredulity (Abrams & Robinson, 2011). Cyberstalking victims may see help seeking as more effective than victims of offline stalking because evidence of the pursuit is easily accessible in written form. These victims mentioned that the recordability and archival of online interactions helped in retrieving evidence that was later given to law enforcement.

Victims of cyberstalking attempted to ignore or avoid the online pursuit, a tactic they found to be moderately effective. Offline stalking victims also commonly avoid or ignore the pursuit by abstaining from interactions with their pursuers and sometimes even avoiding specific physical locations (Bjerregaard, 2000; Blaauw et al., 2000; Brewster, 2002; Fisher et al., 2000; Morrison, 2001). Cyberstalking victims also avoided areas and activities where they would be susceptible to online pursuit, but these locations were digital spaces, such as chat rooms and instant messengers, rather than physical places.

Differences in Managing Offline and Online Stalking

Several tactics unique to the online domain were uncovered in the construction of the cyberstalking management taxonomy. In some cases, victims

engaged pursuers by feigning interest in a relationship or making excuses about why they could not enter into a relationship but would under different circumstances. The physical and psychological distance between cyberstalkers and their victims during pursuit is said to be instrumental in the lowered threat and heightened confidence pursuers feel (Bocij, 2004). It may be that this distance also emboldens victims to behave in ways unintuitive to the cessation of cyberstalking. In offline stalking, victims rarely play along with the pursuit or make excuses for their inability to enter into a relationship because it could contribute to significant risk. These tactics may not even come to mind for victims of offline stalking when asked about risk *management* behaviors. Compliance or excuse-making responses were seen as ineffective means for managing the pursuit.

Tools embedded in a technology can be used effectively to control unwanted online pursuit. Risk management sometimes involved embracing the safeguards built into a technology. Victims deleted old accounts, blocked messages originating from pursuers' accounts, and became more critical about those they accepted as contacts. Often, Internet users are indiscriminate about who they allow to be online contacts because rejecting others accompanies significant social ramifications (boyd, 2004). Nevertheless, victims of cyberstalking became more critical about the online others with whom they associate. They may have also changed their profile pictures, email addresses, and usernames or passwords on their accounts in cases where pursuers were able to obtain such information. In rare cases, victims installed software to protect themselves from future cyberstalking victimization. Victims who had their accounts hacked and their personal information stolen responded by installing malware and antivirus software to protect themselves from further invasion.

Practical Implications

Clinicians, therapists, support centers, law enforcement, and other organizations in cognate areas charged with helping cyberstalking victims can provide them with practical solutions using the findings from this investigation. Victims should be made aware of the large constellation of behaviors used by their predecessors to manage the risks of cyberstalking. To combat pestering forms of cyberstalking, such as hyperintimacy and threat behaviors, victims may consider more passive forms of risk management, such as ignoring or avoiding the pursuit. As the behaviors become more menacing, however, victims should use functions of the technology to move away from their pursuers. Victims can delete old accounts, block pursuers from their contact lists, and change settings on social media profiles to make them more restrictive. Victims might consider combating invasion behaviors by changing usernames and passwords, deleting

email accounts, and installing software that disables pursuers from compromising their computers and accessing private information.

Limitations

The present findings must be interpreted together with the study's limitations. The main findings of this investigation rely on self-report data of the behaviors used in risk management and their perceived effectiveness. First, the university and online sample recruited for this study provided a more complete picture of management tactics used to resolve the large range of cyberstalking behaviors. These data, however, may not be generalizable to the entire population of cyberstalking victims given the strong possibility of self-selection bias among those who responded to the recruitment message. In addition, the online sample found the recruitment letter on two popular websites that supply information about management plans for cyberstalking victimization. This recruitment procedure guarantees that these victims engaged in specific risk management responses, namely, their desire to seek help. More attention in future investigations must be paid to the sampling procedures used to gather data on sensitive issues involving victimization.

Second, victims were asked to evaluate the effectiveness of the behaviors they used to manage cyberstalking. The response effectiveness scale used to assess efficacy of management tactics was based on the presumption that victims necessarily knew what led to the cessation of the cyberstalking behaviors. In many cases, however, victims are never aware of the actual reason why the cyberstalking behaviors ended. The cessation may be attributed to spontaneous remission, a new target, or even lethargy or boredom on the part of pursuers. Future investigations might look at perpetrators' reflections of what behaviors victims undertook that were successful in managing the unwanted online pursuit.

Conclusion

A clearer functional image of cyberstalking perpetration and victimization is emerging as research on the topic continues to mature. This project represents one attempt to catalog the different behaviors used by victims to manage the risks associated with cyberstalking. The results suggest some overlap between the management tactics used by victims of offline and online stalking; however, management behaviors unique to technology use were also identified. Research must continue to answer questions about who is most vulnerable to cyberstalking, whether the channels that cyberstalking occurs through make a difference, and how management tactics vary by the media used to carry out the victimization.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Abrams, K. M., & Robinson, G. E. (2011). Stalking by patients: Doctors' experiences in a Canadian urban area. *Journal of Nervous and Mental Diseases*, *199*, 738-743. doi:10.1097/NMD.0b013e31822fc7aa

Alexy, E. M., Burgess, A. W., Baker, T., & Smoyak, S. A. (2005). Perceptions of cyberstalking among college students. *Brief Treatment and Crisis Intervention*, *5*, 279-289. doi:10.1093/brief-treatment/mhi020

Baker, D. (1999). When cyber stalkers walk. *ABA Journal*, *85*(12), 50-55.

Baum, K., Catalano, S., Rand, M., & Rose, K. (2009). *Stalking victimization in the United States*. Washington, DC: U.S. Department of Justice.

Berkson, J. (1978). In dispraise of the exact test: Do the marginal totals of the 2X2 table contain relevant information respecting the table proportions? *Journal of Statistical Planning and Inference*, *2*, 27-42. doi:10.1016/0378-3758(78)90019-8

Bjerregaard, B. (2000). An empirical study of stalking victimization. *Violence and Victims*, *15*, 389-406.

Blaauw, E., Winkel, F. W., & Arensman, E. (2000, December). *The toll of stalking: The relationship between features of stalking and psychopathology of victims*. Paper presented at the meeting of the Australian Institute of Criminology, *Sydney, Australia*.

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet age and how to protect your family*. Westport, CT: Praeger.

Bocij, P., Griffiths, M., & McFarlane, L. (2002). Cyberstalking: A new challenge for criminal law. *Criminal Lawyer*, *122*, 3-5.

Bocij, P., & McFarlane, L. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal*, *139*, 31-38.

boyd, d. m. (2004). Friendster and publicly articulated social networks. In *Proceedings of ACM Conference on Human Factors in Computing Systems, USA* (pp. 1279-1282). doi:10.1145/985921.986043

Brewster, M. P. (2002). Stalking by former intimates: Verbal threats and other predictors of physical violence. In K. E. Davis, I. H. Frieze, & R. D. Maiuro (Eds.), *Stalking: Perspectives on victims and perpetrators* (pp. 292-311). New York, NY: Springer.

Brzuzy, S., Ault, A., & Segal, E. A. (1997). Conducting qualitative interviews with women survivors of trauma. *Affilia*, *12*, 76-83. doi:10.1177/088610999701200105

Bubas, G. (2001, September). *Computer mediated communication theories and phenomena: Factors that influence collaboration over the Internet*. Paper presented at the meeting of the CARNet Users Conference, *Zagreb, Croatia*.

Cupach, W. R., & Spitzberg, B. H. (2000). Obsessive relational intrusion: Incidence, perceived severity, and coping. *Violence and Victims*, *15*, 357-372.

Cupach, W. R., & Spitzberg, B. H. (2004). *The dark side of relational pursuit: From attraction to obsession to stalking*. Mahwah, NJ: Lawrence Erlbaum.

Dreßing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior, and Social Networking*, *17*, 61-67. doi:10.1089/cyber.2012.0231

D'Ovidio, R., & Doyle, J. (2003). Study on cyberstalking: Understanding investigative hurdles. *FBI Law Enforcement Bulletin*, *72*, 10-17.

Finkelhor, D., Mitchell, K. J., & Wolak, J. (2000). *Online victimization: A report on the nation's youth (No. 6-00-020)*. Alexandria, VA: National Center for Missing and Exploited Children.

Fisher, B. S., Cullen, F. T., & Turner, M. G. (2000). The sexual victimization of college women. Washington, DC: National Institute of Justice and Bureau of Justice Statistics.

Glancy, G. D., Newman, A. W., Potash, M. N., & Tennison, J. (2007). Cyberstalking. In D. A. Pinals (Ed.), *Stalking: Psychiatric perspectives and practical approaches* (pp. 212-226). New York, NY: Oxford University Press.

Goodno, N. H. (2007). Cyberstalking, a new crime: Evaluating the effectiveness of current state and federal laws. *Missouri Law Review*, *72*, 66-102. Retrieved from http://ssrn.com/abstract=1674176

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*, 1-25. doi:10.1080/01639620701876577

Jerin, R., & Dolinsky, B. (2001). You've got mail! You don't want it: Cybervictimization and on-line dating. *Journal of Criminal Justice and Popular Culture*, *9*, 15-21.

Karmen, A. (2012). *Crime victims: An introduction to victimology* (8th ed.). Belmont, CA: Wadsworth.

LeBlanc, J. J., Levesque, G. J., Richardson, J. B., & Berka, L. H. (2001). Survey of stalking at WPI. *Journal of Forensic Sciences*, *46*, 367-369.

Lucks, B. D. (2004). *Cyberstalking: Identifying and examining electronic crime in cyberspace* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3124546)

Lyndon, A., Bonds-Raacke, J., & Cratty, A. D. (2011). College students' Facebook stalking of ex-partners. *Cyberpsychology, Behavior, and Social Networking*, *14*, 711-716. doi:10.1089/cyber.2010.0588

McFarlane, L., & Bocij, P. (2003). An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. *First Monday, 8*, Article 9. Retrieved from http://firstmonday.org/issues/issue8_9/mcfarlane/index.html

Melander, L. A. (2010). College students' perceptions of intimate partner cyber harassment. *Cyberpsychology, Behavior, and Social Networking*, *13*, 263-268. doi:10.1089/cyber.2009.0221

Morrison, K. A. (2001). Predicting violent behavior in stalkers: A preliminary investigation of Canadian cases in criminal harassment. *Journal of Forensic Sciences*, *46*, 1403-1410.

Mullen, P. E., Mackenzie, R., Ogloff, J. R., Pathé, M., McEwan, T., & Purcell, R. (2006). Assessing and managing the risks in the stalking situation. *Journal of the American Academy of Psychiatry and the Law Online*, *34*, 439-450.

Nicastro, A. M., Cousins, A. V., & Spitzberg, B. H. (2000). The tactical face of stalking. *Journal of Criminal Justice*, *28*, 69-82. doi:10.1016/S0047-2352(99)00038-0

Nobles, M. R., Reyns, B. W., Fox, K. A., & Fisher, B. S. (2014). Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly*, *31*, 986-1014. doi:10.1080/07418825.2012.723030

Parsons-Pollard, N., & Moriarty, L. J. (2009). Cyberstalking: Utilizing what we do know. *Victims & Offenders*, *4*, 435-441. doi:10.1080/15564880903227644

Pathé, M., & Mullen, P. E. (1997). The impact of stalkers on their victims. *British Journal of Psychiatry*, *170*, 12-17. doi:10.1192/bjp.170.1.12

Pathé, M., Mullen, P. E., & Purcell, R. (2000). Same-gender stalking. *Journal of the American Academy of Psychiatry and the Law*, *28*, 191-197.

Purcell, R., Pathé, M., & Mullen, P. E. (2000, December). *The incidence and nature of stalking victimization*. Paper presented at the meeting of the Australian Institute of Criminology, *Sydney, Australia*.

Rea, L. M., & Parker, R. A. (1992). *Designing and conducting survey research*. San Francisco, CA: Jossey-Bass.

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for internet users and online place managers. *Crime Prevention & Community Safety*, *12*, 99-118. doi:10.1057/cpcs.2009.22

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*, 1149-1169. doi:10.1177/0093854811421448

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant Behavior*, *33*, 1-25. doi:10.1080/01639625.2010.538364

Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law*, *13*, 627-640. doi:10.1080/10683160701340528

Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology, and stalking. *Violence Against Women*, *13*, 842-856. doi:10.1177/1077801207302045

Spitzberg, B. H., & Cupach, W. R. (1996, August). *Obsessive relational intrusion: Victimization and coping*. Paper presented at the meeting of the International Society for the Study of Personal Relationships, *Banff, Alberta, Canada*.

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society*, *4*, 71-92. doi:10.1177/14614440222226271

Spitzberg, B. H., Nicastro, A. M., & Cousins, A. V. (1998). Exploring the interactional phenomenon of stalking and obsessive relational intrusion. *Communication Reports*, *11*, 33-48. doi:10.1080/08934219809367683

Storey, J. E., & Hart, S. D. (2011). How do police respond to stalking? An examination of the risk management strategies and tactics used in a specialized anti-stalking law enforcement unit. *Journal of Police and Criminal Psychology*, *26*, 128-142. doi:10.1007/s11896-010-9081-8

Strawhun, J., Adams, N., & Huss, M. T. (2013). The assessment of cyberstalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse. *Violence and Victims*, *28*, 715-730. doi:10.1891/0886-6708.11-00145

Suler, J. R. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, *7*, 321-326. doi:10.1089/1094931041291295

Tjaden, P. G. (2014). Stalking and cyberstalking. In J. S. Albanese (Ed.), *The encyclopedia of criminology and criminal justice*. Hoboken, NJ: Wiley. doi:10.1002/9781118517373.wbeccaj446

Tokunaga, R. S. (2011). Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships. *Computers in Human Behavior*, *27*, 705-713. doi:10.1016/j.chb.2010.08.014

Tokunaga, R. S. (2016). Interpersonal surveillance over social network sites: Applying a theory of negative relational maintenance and the investment model. *Journal of Social and Personal Relationships*, *33*, 171-190. doi:10.1177/0265407514568749

Upton, G. J. G. (1992). Fisher's exact test. *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, *155*, 395-402. Retrieved from http://www.jstor.org/stable/2982890

Wall, D. S. (2005). The Internet as a conduit for criminals. In A. Pattavina (Ed.), *Information technology and the criminal justice system* (pp. 77-98). Thousand Oaks, CA: Sage.

Wolke, D., Woods, S., Bloomfield, L., & Karstadt, L. (2000). The association between direct and relational bullying and behaviour problems among primary school children. *Journal of Child Psychology and Psychiatry*, *41*, 989-1002. doi:10.1111/1469-7610.00687

Author Biographies

Robert S. Tokunaga (PhD, University of Arizona) is an assistant professor in the Department of Communicology at the University of Hawai'i at Mānoa.

Krystyna S. Aune (PhD, University of Arizona) is the Dean of Graduate Education at the University of Hawai'i at Mānoa.