Defining Objectives for Preventing Cyberstalking

Gurpreet Dhillon, Chandrashekar Challa, Kane Smith

Defining Objectives For Preventing Cyberstalking

Gurpreet Dhillon[1], Chandrashekar Challa[2], Kane Smith[1]

[1]Virginia Commonwealth University, Richmond, USA
{gdhillon, smithkj6}@vcu.edu
[2]Longwood University, Farmville, USA
challacd@longwood.edu

Abstract. Cyberstalking is a significant challenge in the era of Internet and technology. When dealing with cyberstalking, institutions and governments alike have a problem in how to manage it and where to allocate resources. Hence, it is important to understand how individuals feel about the problem of cyberstalking and how it can be managed in the context of cybersecurity. In this paper we systematically interviewed over 100 individuals to interpret their values on cyberstalking. Keeney's [21] value focused thinking approach is then used to convert individual values into objectives which form the basis for planning to curb cyberstalking and for institutions and governments to allocate resources prudently.

Keywords. Cyberstalking, cyber security planning, values, strategic objectives

1 Introduction

Stalking has been well recognized in the academic and practitioner literature; however with the advent of newer technologies such as social media a new threat has emerged, cyberstalking. An increased reliance of individuals on interpersonal contact has resulted in a corresponding increase in possibility of interpersonal intrusion, referred to as cyberstalking [27]. Institutions and government bodies struggle to manage cyberstalking due to a lack of understanding of the phenomenon. The problem question is twofold: First, what are the objectives to ensure protection against cyberstalking. Second, what priority areas should institutions focus on to ensure that cyberstalking is minimized. In this paper we present a comprehensive set of individual value based objectives which can form the basis for strategic planning to prevent cyberstalking. Theoretically we are informed by the value focused thinking concept purported by Keeney [19]. The paper is organized into five sections: introduction, literature pertinent to cyberstalking, the theoretical and methodological aspects of this research, the fundamental and means objectives for minimizing cyberstalking and finally in the limitations and future research directions.

2 A Review of Existing Cyberstalking Literature

The internet is beneficial in connecting us globally on all fronts and is available in nearly every corner of the globe [17]. It is also the cause of many unique crimes such as cyberstalking because it is cheap, easy to use, and the anonymity it offers in seeking out victims and avoiding detection [22]. Cyberstalking is a type of crime in which there is no face-to-face contact between victims and offenders [10]. According to McFarlane & Bocij [27], there are four types of cyber stalkers: the Vindictive Cyber stalker, the Composed Cyber stalker, the Intimate Cyber stalker and the Collective Cyber stalker.

In the past, cyberstalking victims have not had success in being recognized as victims by law enforcement agencies due to a lack of enforcement training and expertise [34]. A study that analyzes cyber stalking crimes, legislative intervention measures, and preventative initiatives created specifically to curtail this emerging global crime was undertaken by Pittaro [36]. The study concluded that cyberstalking is a serious and growing problem, but proper training and guidance could allow law enforcement agencies can track the stalkers online [22]. However, educating society is still the most effective approach to bringing awareness about cyberstalking and enacting initiatives prevent this Internet based crime. [34]. California was the first state in the USA to adopt stalking laws in 1989 [51]. Since then stalking laws in general have been adopted elsewhere, but cyberstalking is related to one's behavior in cyberspace as opposed to the physical world [3]. Therefore, it is suggested that there should be an investigation of these regulations and ways to adapt new regulations to apply in cyberspace and how these regulations can help prevent cyberstalking.

While cyberstalking is still in its infancy, it is expected to increase significantly as the Internet becomes more popular [16]. For this reason, there are studies such as the one by Spitzberg and colleagues [8, 9, 41, 42, 43] that conducted pilots and introduced the concept of cyber-obsessional pursuit (COP). Further, new research extended these earlier pilot studies to develop and refine measures of cyberstalking victimization [44]. Another study by Goodno [12] examined how differences in state and federal law create gaps in stalking statutes increasing the difficulty in prosecuting all aspects of cyberstalking and suggests ways to close these gaps. Finally, the study also examines the potential issues in criminalizing cyberstalking and how these issues might be resolved by changing the laws so they address the newer cyber security crimes as a result of cyberstalking. Additional work with respect to cyberstalking has sought to develop and adapt a

lifestyle–routine activities theory [38] to explain opportunities for victimization in cyberspace environments where traditional conceptions of time and space are less relevant. A related earlier study on the extent and nature of Cyberstalking victimization from a lifestyle/routine activities perspective by Reyns [37] also corroborates the theory. Findings from this study indicate that the number of differing factors such as the number of online social networks an individual owns or low self-control are significant predictors of cyberstalking victimization, suggesting moderate support for lifestyle/routine activities theory in explaining cyberstalking [37].

3 Methodology

In order to identify values one must ask the concerned people [21]. Within the literature, there is a significant variance in the number of individuals that should be interviewed. As an example, Hunter [15] used the interviews of 53 people from two different organizations to do a content analysis to elicit individual conceptions. However, Phythian & King [35] used two managers who were experts in assessing tender enquiries to identify key factors and rules that influence tender decisions. Additionally, Keeney [21] obtained interviews from over 100 individuals to obtain their values to develop objectives that influenced Internet purchases. For this study, over 100 persons of varying background and experience were interviewed to identify general values for managing cyber stalking related information security.

The following three-step process is used to identify and organize the values that an individual might have with respect to cyberstalking [19]: First, interviews are conducted which elicit the values an individual might have within a decision context. Second, individual values and statements are converted into a common value format, such as an objective oriented statement. Then similar objectives are grouped together in order to form clusters of objectives. Finally, the objectives are then classified as either fundamental to the decision context, resulting in a fundamental objective, or simply a means to achieve the fundamental objectives, or what's called a means objective.

3.1 Identifying values

To begin, interviews are conducted with the concerned peoples as a process of identifying values. At the beginning of each interview, the purpose is clarified and context and scope of the interview are established. The core objective is to

understand the fundamental objectives for preventing cyberstalking. To set the decision context, we emphasize that the scope for eliciting these values is limited only to individuals. After defining the scope of the interview, explanations are provided to the interviewee so that they can understand what 'cyberstalking' is to establish a common understanding. Cyberstalking is thusly defined as 'the use of the internet, email, or other electronic communications devices to stalk another person' [48]. It is made clear to respondents that the goal is to understand values that people might have with respect to cyberstalking. To identify these values four questions are posed about their personal values toward cyberstalking and those of individuals who commit acts of cyberstalking. The questions were: What do you think are your values and wishes in order to prevent cyberstalking? What values might lead you to behave in a certain manner towards cyberstalking? What kind of information do you think people use to engage in cyberstalking? What personal values lead people to use this information for their own benefit while cyberstalking? All questions were open-ended. As individuals can express values differently, so difficulty exists with the quiescent nature of the values, so different probing techniques are used to identify latent values. Keeney [19] suggests words like trade-offs or consequences etc. as useful in making implicit values explicit.

3.2 Structuring values

Once values have been identified, value structuring and objectives development begins. Step one is that all statements are restated in a common form with duplicates are removed, then common form values are considered and converted into sub-objectives. According to Keeney [21], an objective is constituted of the decision context, an object and a direction of preferences, which in this case is cyberstalking. With all values systematically reviewed and converted into sub-objectives a number of sub-objectives that deal with a similar issue exists. By carefully reviewing the content of each of these sub-objectives, clusters are developed that group similar ones together and then each cluster of sub-objectives is labeled by its overall theme that becomes the main objective.

3.3 Organizing objectives

The list of sub-objectives and corresponding clusters initially include both means and fundamental objectives so we must differentiate the two. This is accomplished by repeatedly linking objectives through means–ends relationships then specifying the fundamental objectives. To identify fundamental objectives, the question is asked, 'Why is this objective important in the decision context?

[19].' If the objective is an essential reason for interest in the decision context, then the objective is a candidate as a fundamental objective. If the objective is important due its implications with respect to some other objective, then it is a candidate as a means objective. This is termed by Keeney [20] as the 'WITI test.'

4 Objectives for Preventing Cyberstalking

In this section we present fundamental and means objectives for preventing cyberstalking. In our research we found twenty total objectives: five fundamental objectives and fifteen means objectives. In this section we discuss the fundamental and means objectives and how these can collectively contribute to the prevention of cyberstalking.

4.1 Fundamental Objectives for Preventing Cyberstalking

The five fundamental objectives identified in this research include: Protecting Online Interactions; Establishing cyberstalking security procedures, Ensuring technical security, Developing strong value systems and Defining intermediaries to minimize cyberstalking. The fundamental objectives resonate well with what has been defined in the literature and the main characteristic for cyberstalking - repeated event, invasion of personal privacy, evidence of threat and/or fear [44]. Scholars term stalking as a form of *Obsessive Relational Intrusion* (ORI), which is the unwanted pursuit of intimacy [8,9].

FO1 Protecting Online Interactions. Respondents found protection of online interactions to be defined as both precautionary and regulatory objectives. Exercising caution when meeting people online is fundamental, however it is also important to ensure that protection mechanisms exist in online forums; however the means are addressed in some of our means objectives. A response by one respondent noted: "It is the responsibility of Internet Companies to ensure safety in an online forum through regulation and technical means." In an interesting paper, Chik [6] discusses international cyberstalking regulatory considerations. He notes that there are two basic types of anti-stalking legislations - the list model and the closed model. The list model lists types of offences and provides certainty, but is rather restrictive. An alternative is the general prohibition model, which is used in some US states and UK. Chik argues that the more open general prohibition model is the favored option [6].

FO2 Establishing cyberstalking security procedures. Respondents felt that good cyberstalking security procedures will go a long way in ensuring security and safety. Cyberstalking security procedures can include an identification of appropriate authentication measures or availability of cyberstalking prevention tools. A respondent noted: "There is no way to tell which site provides adequate security and which one has loose controls, I wish we had a way to do this." Website trustworthiness is an important topic area and has been well researched. At the advent of e-commerce, online vendors were facing similar challenges. Moores and Dhillon [29] found that web assurance seals did help in ensuring a trusting relationship with the consumers. They note: "The relative success of the privacy seals suggests that many sites recognize the issue of privacy and strive to uphold the highest standards. These sites are not the problem. The problem is with those sites that violate their stated obligations, those sites that make no commitment, and those sites that actively seek to exploit the data they collect."

FO3 Ensuring technical security. The role of technologies in ensuring security in cyberstalking cannot be underestimated. Unequivocally our respondents made a call for investing in safe browsing technologies and increased abilities to monitor online security settings. Ability to create online filters to block negative behavior was also considered important. One respondent noted: "Now-a-days it is virtually impossible to ensure that the filters are installed properly. People need a high level of competence. Why can't the technologies be made simple and easy to use?" Technical means to ensure online security and its benefits in preventing cyberstalking incidents has been noted by Goldberg [11], who summarizes the problem as one dealing with secure Internet routing. Goldberg notes that secure Internet routing can be achieved through simple cryptographic whitelisting techniques, which can prevent attacks such as prefix hijacks, route leaks, and path-shortening attacks. Some of these attacks are the basis for website compromises, which can then subsequently lead to increased incidents of cyberstalking.

FO4 Developing strong value systems. Early detection of negative behaviors can come about through strong family values and the related social pressures. In a study by Pereira and Matos [33] the complexity of family values is reviewed as well as their impact on cyberstalking. In particular Pereira and Matos found fear following victimization plays a major role in management of cyberstalking [33]. One respondent noted: "I have been cyberstalked. Support from my family was critical in helping me carry on with life."

FO5 Defining intermediaries to minimize cyberstalking. This fundamental objective is somewhat related to the fundamental objective of ensuring secure procedures. Critical to trust forming relationships is the role of intermediaries. Cybersecurity insurance research has suggested that it is indeed possible to minimize threats by appropriately focusing on insurance practices. Pal et al [32] note: "To alleviate this issue a security vendor can enter the cyber-insurance ecosystem and via a symbiotic relationship between the insurer can increase its profits and subsequently enable the cyber-insurer to always make strictly positive profits keeping the social welfare state identical. As a special case the security vendor could be the cyber-insurer itself (p. 8)."

4.2 Means Objectives for Preventing Cyberstalking

MO1 Increase responsibility of social media sites. This objective pertains to organizations responsible for creating, maintaining, regulating and implementing social media sites. These organizations have an obligation to ensure their sites are safe in order to prevent cyberstalking. Many organizations consider this a corporate social responsibility (CSR) and make efforts to shape CSR policies to present themselves as good corporate citizens [28] and the importance of CSR has been emphasized by many in the literature [5].

MO2 Increase safe information sharing. This objective addresses the need for users to have more tools to safely share information on the Internet and social media sites can provide those tools. Types of tools that could be included are increased privacy settings or private web browsing methods. Responses indicate support for this belief such as; "I want more privacy settings and ways to protect my information if I choose to share it."

MO3 Increase law enforcement. This objective deals with ensuring useful laws exist to protect online users from cyberstalking. One study analyzed was the police use of Twitter, including the structure of networks and the content of the messages [7]. The study concluded that due to the constraints of police culture, Twitter has been used cautiously as reinforcement for existing means of communication [7]. Responses such as; "law enforcement needs to be more involved in monitoring and policing social media activity" show users want an active law enforcement approach to help prevent cyberstlaking.

MO4 Increase awareness of cyberstalking consequences. This objective addresses the consequences for cyberstalking, specifically making people aware

of the negative effects on victims and society as a whole. A survey response supporting this is "as a society we need to increase awareness about the harmful effects of cyberstalking" which speaks to the lack of awareness.

MO5. Minimize trolling. This objective deals with discouraging people from posting offensive content in their online postings. A study by Hopkinson [14] researched the practice of trolling in online discussion forums and its findings suggest that the definition of trolling varies depending on the discussion topic [14]. The study found a paradoxical view of trolling in that it is considered destructive and have a negative connotation, but cases exist where it can have a positive constructive effect [14].

MO6 Decrease tracking ability. This objective deals with ensuring that your current location is unknown to people from whom you wish to remain hidden from. For example, Facebook had a program, which sent messages to users' friends about what they were buying on Web sites; it had to retract this feature after protest from a number of their users due to complaints about sharing without permission [45]. To prevent features like these from being abused for cyberstalking, the ability of companies and individuals to track people online needs to be minimized.

MO7 Increase deterrence. This objective deals with the use of punishment as a threat to stop or prevent people from engaging in cyberstalking. Individuals behave rationally to maximize their utility and commit crime when the expected utility of law breaking far exceeds the expected disutility of punishment [18]. So to promote obedience and discourage crime communities should adopt a policy to raise the price of crime. Deterring cyberstalking was a common response, for example, one of our respondents said; "Well-defined laws and stricter enforcement of cyber stalking laws would help prevent cyberstalking."

MO8 Ensure online social responsibility. Organizations and individuals alike have a significant stake in achieving this objective to prevent cyberstalking. There are conflicting views from certain studies whether "Doing Good Always Leads to Doing Better" [39]; however organizations and individuals should proactively take responsibility for making online experiences positive by following basic and fundamental norms of conduct and behavior.

MO9 Personal accountability. Accountability protects public health and safety, facilitates law enforcement, and enhances national security, but it is more than a

bureaucratic concern for corporations, public administrators, and the criminal justice system [2]. In our study we found that respondents have given significant importance to this aspect where one respondent said, "I believe each person is responsible for taking steps towards preventing cyberstalking. That means being mindful of what personal information you share about yourself on the Internet."

MO10 Increase ability to control personal information. Users desire the ability to control their personal information; how it is shared, stored and distributed over the Internet. Information available online about consumers is striking and the media is filled with horror stories about the misuse of personal information, such as the availability of information most people consider confidential like social security numbers or their home location [40]. Many respondents felt this way with one responding; "I want as many options on social media as possible to prevent as much personal information from being publicly available."

MO11 Ensure monitoring of children. This objective deals with the ability to monitor children's online activity and behavior. This is a difficult objective that is highly complex. For example, a national study in Great Britain on children and their parents used focus group interviews and observation of children's use of the internet to reveal the following: Parents seek to manage their children's internet use, but face challenges in helping their children use internet safely. Disagreement between parents and children exists as most children do not want restrictions and have take measures to hide their online activity from their parents demonstrating a gap in the understanding between parents and children on these issues [25]. Their policy recommendations were; direct children and young people towards valuable content, develop online advice resources with young people etc. [25].

MO12 Reduce opportunities for online victimization. This objective emphasizes the importance of safe browsing and online behavior in order to reduce the opportunity an offensive act can be undertaken by someone. For example, cyberbullying is one major issue in schools and communities due to the emotional, psychological, and even physical harm to which victims can be subjected. One study looked at general strain theory to identify the emotional and behavioral effects of cyberbullying victimization [13]. Data collected indicated that cyberbullying is a potent form of stress that may be related to school behavior problems and delinquent behavior offline **[**13]. Another study from a national survey of teenagers in the UK (N=789) analyzed the demographic factors that influence skills in using the Internet and then sought to determine whether these skills make a difference to online opportunities and online risks [26]. Findings

show that those who take up more opportunities encounter more risks and vice versa. Further, those groups inclined to gain more opportunities also encounter more risks [26].

MO13 Increase Regulation of Online Social Networks. This objective deals with agencies and government organizations monitoring online social networks and determining the rules and actions that need to be taken to prevent cyberstalking. One study investigated a sample (n = 704) of college students to understand online disclosure and withdrawal of personal information [47]. Findings show little to no relationship between online privacy concerns and information disclosure on online social network sites as students manage unwanted audience concerns by adjusting profile visibility and using nicknames but not by restricting the information within the profile [47]. This behavior suggests that people can still easily gain access to all the free information on Internet, hence why our study suggests social network organizations adopt various counter-measures.

MO14 Increase mental health screening. Mental health can adversely influence one's ability and judgment to conduct themselves properly online. A survey study of 371 British students showed that 18.3% of the sample was considered to be pathological Internet users, whose excessive use of the Internet was causing academic, social, and interpersonal problems [30]. This would lead one to consider that Internet usage, cyberstalking and mental health are a connected and important area of concern.

MO15 Cyberstalking education. Cyberstalking and its negative affects are not well known to many people. One study of note was done using students from two universities, which gathered their responses to a cyberstalking scenario as well as their use and experiences with the Internet [1]. Then the study conducted an analysis and comparison of students who reported having been stalked to those who had been cyberstalked [1]. An interesting finding was that male students were statistically more likely than female students to have been cyberstalked [1]. Additionally, for individuals who were cyberstalked, the stalking perpetrator was most likely to be a former intimate partner [1].

5. Further research, Limitations and Conclusions

Based on the research presented in this paper, there are three broad categories, which exist for future research opportunities. The first opportunity is that the list

of objectives identified in this research can be subjected to psychometric analysis using separate large samples. This can help, for example, in developing a model for measuring cyberstalking by organizations on social media sites. A second opportunity exists for intensive research to be undertaken to establish relationships between particular fundamental and means objectives; however, while Keeney [19] contends that fundamental and means objectives are related and an implicit; logical relationships appear to exist between the fundamental and means objectives, but specific relationships need to be researched. The final opportunity is such that further quantitative work should be carried out to assess how the subscales of means and fundamental objectives relate to each other.

The findings of this research lay a suitable foundation for developing multidimensional measures and protections against cyberstalking. For example, Keeney [21] conducted an extensive study, which interviewed over 100 people to assess their values with respect to Internet commerce. And based on this work, Torkzadeh & Dhillon [46] were then able to develop instruments, which measured factors that influence Internet commerce success. Much in the same way, the research presented within this paper has established values and objectives that would be a basis for measures and protections against cyberstalking. Within the IS domain, many examples exist of research that involves in-depth qualitative research aimed at the development of theoretical concepts which includes research on organizational consequences of IT [31], relationship between IS design, development and business strategy [49] and communication richness [24].

In the cybersecurity field, the topic of cyberstalking is constrained by the absence of well-grounded concepts that are developed in a systematic and a methodologically sound manner as the topic itself is still a newer concept. The fundamental and means objectives that are presented in this paper make a contribution towards the development of theory specific to cyberstalking and measures and protections from it, a largely overlooked IS research stream. This research was only the first step to identify means and fundamental objectives as it relates to cyberstalking values. The next step in this research is to conduct a quantitative study as was done earlier by Torkzadeh & Dhillon [46] to come up with an instrument that measures fundamental objectives as it relates to cyberstalking as there is a need to develop theory that is IS specific [4].

As with most qualitative research, this study is subject to some limitations. The process of identifying values from interview data is largely subjective and interpretive and while as researchers we maintain a professional distance, there is

always a possibility that some of our own biases may influence the results; however, we were conscious of this during all three phases. The previous basis for this research and the critical reflections of the interviewee's statements was useful in helping us show how these various interpretations emerged in the research [23]. For this reason, it is believed that being aware of the intellectual biases actually helped us to be objective within our analysis of the data. Further, Walsham [50] recognized this to be an issue when carrying out intensive research and in regard to the role of the researcher wrote; "the choice should be consciously made by the researcher dependent on the assessment of . . . merits and demerits in each particular case (p. 5)." It is our goal that in strictly following the value-focused thinking method and being conscious that our interpretations should not serve to influence our research, it can provide confidence in the outcome of this study.

In conclusion, the research presented in this paper examines the relatively unexplored area of cyberstalking in the field of information systems. This qualitative investigation, which used value-focused thinking, revealed 75 sub-objectives, grouped into five fundamental and 15 means objectives, which are essential for developing measures and protections against cyberstalking. The objectives developed in this study are grounded socio-organizationally and provide a way forward in developing measures and protections against cyberstalking. Therefore, this is a significant contribution as previous research in this area is underdeveloped and as such falls short of being able to propose tangible measures and protections against cyberstalking.

References

[1] Alexy, Eileen M., (2005) "Perceptions of cyberstalking among college students." *Brief Treatment and Crisis Intervention* 5.3: 279.

[2] Allen, Anita L. (2003) Why privacy isn't everything: Feminist reflections on personal accountability. Rowman & Littlefield.

[3] Basu, S. and Jones, R.P. (2007), "Regulating Cyberstalking", Journal of Information, Law and Technology.

[4] Benbasat, I. (2001) Editorial note. Information Systems Research, 12, iii–iv

[5] Bauer, Theresa (2014), The Responsibilities of Social Networking Companies: Applying Political CSR Theory to Google, Facebook and Twitter, in Ralph Tench, William Sun, Brian Jones (ed.) Communicating Corporate Social Responsibility: Perspectives and Practice (Critical Studies on Corporate Responsibility, Governance and Sustainability, Volume 6) Emerald Group Publishing Limited, pp.259 - 282.

[6] Chik, W. (2008). Harassment through the Digital Medium-A Cross Jurisdictional Comparative Analysis of the Law on Cyberstalking. *J. Int'l Com. L. & Tech.*, *3*, 13.

[7] Crump, J. (2011) What Are the Police Doing on Twitter? Social Media, the Police and the Public; " Policy & Internet: Vol. 3: Iss. 4, Article 7.

[8] Cupach, W. and B. Spitzberg (1998) 'Obsessive Relational Intrusion and Stalking', in B. Spitzberg and W. Cupach (eds) The Dark Side of Close Relationships, pp. 233–63. Hillsdale, NJ: Erlbaum.

[9] Cupach, W. and B. Spitzberg (2001) 'Obsessive Relational Intrusion: Incidence, Perceived Severity, and Coping', Violence and Victims 15(1): 1–16.

[10] Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach (Crime Prevention Studies, Vol. 16, pp. 7-39). Monsey, NY: Criminal Justice Press.

[11] Goldberg, S. (2014). Why is it taking so long to secure Internet routing?. *Communications of the ACM*, *57*(10), 56-63.

[12] Goodno, N. H. (2007) Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws; Missouri Law Review, Vol 72, Issue 1.

[13] Hinduja, Sameer, and Justin W. Patchin. (2007) "Offline consequences of online victimization: School violence and delinquency." *Journal of school violence* 6.3: 89-112.

[14] Hopkinson, C. (2013) Trolling in Online Discussions: From Provocation to Community-building; Brno Studies in English Volume 39, No. 1.

[15] Hunter, M.G. (1997) The use of RepGrids to gather data about information systems analysts. Information Systems Journal, 7, 67–81.

[16] Hutton, S. (2003). Cyber stalking. Retrieved Feb. 18, 2006, from National White Collar Crime Center Web site: http://www.nw3c.org.

[17] Jaishankar, K., & Uma Sankary, V. (2005). Cyber stalking: A global menace in the information superhighway. ERCES Online Quarterly Review, 2(3), Retrieved May 7, 2007, from http://www.erces.com/journal/articles/archives/volume2/v03/v02.htm.

[18] Kahan, Dan M. (1997) "Social Influence, Social Meaning, and Deterrence". Virginia Law Review 83.2: 349–395.

[19] Keeney, R.L. (1992) Value-Focused Thinking. Harvard University Press, Cambridge, MA, USA

[20] Keeney, R.L. (1994) Creativity in decision making with value-focused thinking. Sloan Management Review, 35, 33–41.

[21] Keeney, R.L. (1999) The value of Internet commerce to the customer. Management Science, 45, 533–542

[22] Reno, J. (1999). 1999 report on cyberstalking: A new challenge for law enforcement and industry. Retrieved Feb. 18, 2006, from US DOJ Web site: http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm.

[23] Klein, H.K. & Myers, M.D. (1999) A set of principles for conducting and evaluating interpretive field studies in information systems. MIS Quarterly, 23, 67–94.

[24] Lee, A.S. (1994) Electronic mail as a medium for rich communication: an empirical investigation using hermeneutic interpretation. MIS Quarterly, 18, 143–157.

[25] Livingstone, Sonia, and Magdalena Bober. (2005) "UK children go online: Final report of key project findings."

[26] Livingstone, Sonia, and Ellen Helsper. (2009) "Balancing opportunities and risks in teenagers' use of the Internet: The role of online skills and Internet self-efficacy." *New media & society*.

[27] McFarlane, L., & Bocij, P. (2005). An exploration of predatory behavior in cyberspace: Towards a typology of cyber stalkers. First Monday, 8. Retrieved Feb 18, 2006, from http://firstmonday.org/issues/issues8_9/mcfarlane/index.html.

[28] Melissa, J.R. (2009) Why Social Media Is Vital to Corporate Social Responsibility; http://mashable.com/2009/11/06/social-responsibility/#lL17q023Caqh.

[29] Moores, T. T., & Dhillon, G. (2003). Do privacy seals in e-commerce really work?. *Communications of the ACM*, *46*(12), 265-271.

[30] Niemz, Katie, Mark Griffiths, and Phil Banyard. (2005) "Prevalence of pathological Internet use among university students and correlations with self-esteem, the General Health Questionnaire (GHQ), and disinhibition."*CyberPsychology & Behavior* 8.6: 562-570.

[31] Orlikowski, W.J. & Robey, D. (1991) Information technology and structuring of organizations. Information Systems Research, 2, 143–169.

[32] Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2014). Will cyber-insurance improve network security? A market analysis. In *INFOCOM, 2014 Proceedings IEEE* (pp. 235-243). IEEE.

[33] Pereira, F., & Matos, M. (2015). Cyber-Stalking Victimization: What Predicts Fear Among Portuguese Adolescents?. *European Journal on Criminal Policy and Research*, 1-18.

[34] Petrocelli, J. (2005). Cyber stalking. Law & Order, 53(12), 56-58.

[35] Phythian, G.J. & King, M. (1992) Developing an Expert System for tender enquiry evaluation: a case study. European Journal of Operational Research, 56, 15–29.

[36] Pittaro, Michael. (2007). Cyber stalking: An Analysis of Online Harassment and Intimidation; International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 Vol 1 (2): 180–197

[37] Reyns, B.W. (2010) Being Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective; A Dissertation Submitted to the: Graduate School of the University of Cincinnati

[38] Reyns, B.W., Henson,B, & Fisher, B.S. (2011) Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization; Criminal Justice and Behavior, Vol. 38 No. 11.

[39] Sankar Sen, C.B. Bhattacharya (2001) Does Doing Good Always Lead to Doing Better? Consumer Reactions to Corporate Social Responsibility. Journal of Marketing Research: May 2001, Vol. 38, No. 2, pp. 225-243.

[40] Sovern, Jeff. (1999) "Opting in, opting out, or no options at all: The fight for control of personal information." Wash. L. Rev. 74: 1033.

[41] Spitzberg, B., A. Nicastro and A. Cousins (1998) 'Exploring the Interactional Phenomenon of Stalking and Obsessive Relational Intrusion', Communication Reports 11(1): 33–48.

[42] Spitzberg, B. and J. Rhea (1999) 'Obsessive Relational Intrusion and Sexual Coercion Victimization', Journal of Interpersonal Violence 14(1): 3–20.

[43] Spitzberg, B., L. Marshall and W. Cupach (2001) 'Obsessive Relational Intrusion, Coping, and Sexual Coercion Victimization', Communication Reports 14(1): 19–30.

[44] Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. New media & society, 4(1), 67-92.

[45] Story, L. & Stone, B. (2007); Facebook Retreats on Online Tracking; www.nytimes.com

[46] Torkzadeh, G. & Dhillon, G. (2002) Measuring factors that influence the success of internet commerce. Information Systems Research, 13, 187–204.

[47] Tufekci, Zeynep. (2008) "Can you see me now? Audience and disclosure regulation in online social network sites." *Bulletin of Science, Technology & Society* 28: 20-36.

[48] US Attorney General (1999) 'Cyberstalking: A New Challenge for Law Enforcement and Industry', Report from the Attorney General to the Vice President

[49] Walsham, G. & Waema, T. (1994) Information systems strategy and implementation: a case study of a building society. ACM Transactions on Information Systems, 12, 150–173.

[50] Walsham, G. (1995) Interpretive case studies in IS research: nature and method. European Journal of Information Systems, 4, 74–81.

[51] Zona, M.A., Sharma, K.K., & Lane, M.D. (1993) "A Comparative Study of Erotomanic and Obsessional Subjects in a Forensic Sample" Journal of Forensic Sciences, 38, p. 894– 903