Important Issues for Preventing Cyberstalking in India

Emergent Research Forum (ERF) Paper

Kane J. Smith
University of North Carolina at Greensboro
Kjsmith9@uncg.edu

Gurpreet Dhillon
University of North Carolina at Greensboro
Gdhillon@uncg.edu

Ella Kolkowska
Orebro University
ella.kolkowska@oru.se

Abstract

Cyberstalking is a significant and highly challenging problem in the era of Internet and technology. When dealing with cyberstalking, both institutions and governments share in the problem of how to manage it and where to allocate resources in the context of security and privacy. Hence, it is important to understand how individuals affected by Cyberstalking feel about the problem and how it can be managed in the context of cybersecurity. This issue is especially pronounced in India where cyberstalking has become a pervasive menace and solutions are urgently required. Therefore, in this paper we conduct a Delphi study to explore the security and privacy concerns of both men and women in India in order to understand differences and commonalities of the two groups. The goal is to illuminate the preferred cybersecurity prevention methods of men and women in India which can ultimately lead to the creation of more effective policy.

Keywords

Cyberstalking, Policy Development, Delphi Study

Introduction

There is a great deal of both academic and practitioner literature, which recognizes the concept of stalking. However, due to the increased reliance on information and communication technologies, particularly social media, a new threat of cyberstalking has emerged. The incredible rise and proliferation of social media has significantly increased online interpersonal contact. According to McFarlane & Bocij (2005) this increase in interpersonal contact has resulted in an increase in the possibility of a form of interpersonal intrusion. McFarlane & Bocij (2005) state that this type of violation of one’s privacy and security is known as cyberstalking. As this form of interpersonal intrusion is still relatively new, both governments and institutions are struggling to understand and respond to this problem. The issue of cyberstalking has become extremely important in India as in the last 5 years alone the country has seen an explosion of growth amongst internet connected users, averaging ~37% YoY growth, greatly increasing the potential for interpersonal intrusion (internetlivestats.com). This incredible level of growth in internet use makes cyberstalking an important issue for the government and institutions within India to understand the security and privacy concerns of its citizens with respect to cyberstalking. This is due to India seeing a dramatic increase in cyberstalking, but has been unable to respond effectively. According to the BBC (Roy 2015) India passed the Information Technology Act of 2000, which intended to help prosecute cases of cyberstalking. Unfortunately, while numerous reports have been made of cyberstalking reported under the act, only recently in 2015, has its first offender actually been prosecuted (Roy 2015). Cyberstalking crimes committed in India have grown more violent as well with harassment becoming common (Roy 2015). For example, Nobel laureate Amartya Sen sent a tweet that resulted in prolonged cyberstalking by anonymous twitter users who sent him threats of death and rape, violating his privacy and threatening his security (Roy 2015). It is due to this growing problem of cyberstalking in India that
this paper seeks to address the problem from the perspective of what women and men in India would like to see done to prevent cyberstalking. Therefore the problem question is twofold: First, What are the key issues for preventing cyberstalking in India for both men and women. Second, to what extent there is convergence of current cyberstalking policy and the issues presented in this study for men and women in India. In this paper we explore the first research question by conducting a Delphi study using the methodological blueprint provided by Schmidt (1997) to guide the research process and discover the issues pertinent to men and women in India. The paper is organized as follows: introduction, literature pertinent to cyberstalking, research design and methodology, sample results, and finally a discussion of future research directions and conclusion.

**Literature Review**

Research related to privacy and security concerns within the context of cyberstalking tend to fall into three broad categories - issues of legality and regulation in cyberstalking, characteristics of cyberstalking and the societal impact of cyberstalking. Each category generally addresses a different fundamental dynamic of the overall cyberstalking thematic. The categorizations of the associated literature presented here are only for the purpose of this paper.

Issues of Legality and Regulation in Cyberstalking is perhaps the largest category found in the cyberstalking literature. There are numerous articles discussing various topics such as; the effectiveness of current state and federal laws with regard to cyberstalking (Goodno 2007), identifying relevant themes in existing legislation that pertains to cyberstalking (Hazelwood & Koon-Magnin 2013) and Jurisdictional and definitional concerns of cyberstalking crimes (Roberts 2008). A major thematic which can be synthesized from the work in this category is that it attempts to define cyberstalking, establish legal boundaries and frameworks for the criminalization of cyberstalking and identify which laws and regulations already in existence may pertain to cyberstalking activities. This is relevant to address in our research as we use already established understandings of cyberstalking to contextualize our study with participants. We also aim to provide useful insight to research conducted in this area such that policymakers who intend to design effective laws and regulations regarding cyberstalking can address the concerns of those most directly affected. Hence, we believe the incorporation of privacy and security concerns regarding cyberstalking elicited in this study will enhance the efficacy of the aforementioned laws and regulations.

Characteristics of Cyberstalking is an important category as it attempts to explain the characteristics of this deviant behavior. For example, there are studies such as the one by Spitzberg and colleagues (Cupach & Spitzberg 1998; Cupach & Spitzberg 2001; Spitzberg et al 1998; Spitzberg & Rhea 1999; Spitzberg et al. 2001) that conducted pilots and introduced the concept of cyber-obsessional pursuit (COP) in order to explain deviant behavior. This category is important to our study in the following ways: First, it helps establish the boundaries for our sample selection and second, it allows us to further contextualize the characteristics of cyberstalking on which our study should focus. This means that it aids us in establishing a profile for cyberstalking behavior as well as contextualizes how men and women are affected differently by the behavior and as such, may respond differently to questions about how to prevent it. It is important to note that men and women are indeed different with respect to cyberstalking demonstrated by the literature in this category and our sample selection stands on this preface.

Societal Impact of Cyberstalking is likely the least represented category of cyberstalking related literature. Nevertheless it is an important aspect of research, which is quite distinct from the previous two categories. While the first two categories look at legal aspects or victim/stalker characteristics related to cyberstalking, this category deals specifically with the societal impact of cyberstalking. This means that research in this category looks at cyberstalking’s impact on society as a whole, including organizations and the government, not just at individuals. For example, a study by Tavani & Grodzinsky (2002) looked at issues involving moral responsibility for Internet service providers (ISPs) when stalking crimes occur in their ‘space’ on the Internet. This category is explicitly linked to our research in that the underlying purpose of this work is to enhance societies understanding of privacy and security concerns regarding cyberstalking and to highlight mechanisms by which both governments and organizations can improve their laws, regulations and policies. As the purpose of this work is to highlight cyberstalking’s measurable impact on society, it serves to further reinforce and validate the need for this type of research.
Important Issues for Preventing Cyberstalking in India

Research Design & Methodology

In this research we use the Delphi method to identify important societal concerns pertinent to the prevention of Cyberstalking amongst men and women in India. The objective of this study is to develop a comprehensive list of concerns in India related to preventing Cyberstalking. The Delphi method is a suitable way to elicit such issues as opinions of the participants through iterative feedback-based convergence and, identify and rank the concerns in order of importance. The Delphi method has some distinct advantages over other ranking methods, which is discussed by Okoli and Pawloski (2004) who describe the strengths and weaknesses of Delphi method with respect to other ranking approaches. In this study, we applied the Delphi method for the following three reasons: One, the Delphi method allows to inquire and seek the divergent opinions and experiences of different participants affected by cyberstalking and translate those into a reliable and validated list of security and privacy concerns for both governments and institutions in India. Two, we employed a ranking method based on Schmidt’s Delphi methodology to elicit opinions of panels of Indian men and women through controlled inquiry and feedback (Schmidt 1997). Delphi study allowed security and privacy concerns over cyberstalking to converge to the ones that are important for men, women and men and women. Three, the Delphi method allows understanding of the complex issue of cyberstalking from the perspectives of both men and women in India. Participants were selected based on the context of the study, determining the security and privacy concerns of men and women in India with respect to the prevention of cyberstalking. Therefore a sample of both men (N= 12-15) and women (N= 9-12) was selected from the population, which was consistent in demographics of an urban setting in India. All our participants were in the 20-29 age group and lived in Bangalore. We selected our sample carefully as these categories represent the predominant demographics of internet users in India. Rural India does not yet possess the high rates of Internet users and the resulting interpersonal intrusions regarded as cyberstalking. Hence, it is important for the purpose of this study to select the persons most likely to be affected by cyberstalking and make comparisons amongst only the relevant groups. Additional age groups were not considered as older generations of Indian society make up only a very small portion of Internet users. Hence, younger and more engaged users who represent the vast majority of people most likely to be affected were selected. Additionally, the literature on cyberstalking (Cupach & Spitzberg 1998; Cupach & Spitzberg 2001; Spitzberg et al 1998; Spitzberg & Rhea 1999; Spitzberg et al. 2001) suggests that there are differences between men and women and as such we desired to explore these potential differences based on the literature. Further, our sample size conforms to the suggestions made by other scholars. For example, Schmidt (1997) suggests these studies limit the number of participants to between 9 and 12, prevent them from being intimidated with feedback generated during ranking rounds. Likewise, Okoli and Pawlowski (2004) recommend a group size of 10 to 11 as the results are dependent on group dynamics rather than group size. Furthermore, the participants in this study represented a typical Indian urban population.

In line with Schmidt (1997) three distinct phases occurred during the process of the data collection: First, in the discovery of issues participants were solicited as to their preferences for preventing cyberstalking. Second, a review occurred where a determination was made as to the most important issues. Lastly, the issues were ranked by the men and women in the study to ascertain their preferred importance. Within the first and third phase of the study, several rounds were conducted, however the second phase only required one round to achieve the desired results. Additionally, Kendall’s coefficient of concordance (W) is used in each round to measure agreement amongst participants. Kendall’s method measures current agreement (the ordered list by mean ranks) with a least squares solution and is the most popular method for this purpose, mainly due to its simplicity of application for ranks. It calculates agreements between 3 or more rankers as they rank a number of subjects according to a particular characteristic. The idea is that N subjects/topics are ranked (0 to n-1) by each of the rankers, and then statistics are used to evaluate how much the rankers agree with one another.

Delphi Study Data Sample of Cyberstalking Issues

The following tables (See Table 1 & 2) are samples of the Male and Female issues in India developed by this study.

<table>
<thead>
<tr>
<th>No</th>
<th>Issues (11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Maintain security in your system: use of good and updated security software, assure that the security software has internet security service as well</td>
</tr>
<tr>
<td>2</td>
<td>Increase awareness about cyberstalking in the society: educate an individual about Cyberstalking, media can</td>
</tr>
</tbody>
</table>

Twenty-fifth Americas Conference on Information Systems, Cancun, 2019
Important Issues for Preventing Cyberstalking in India

1. Maintain security in your system: use of good and updated security software, renew your antivirus, always use updated software which assures maximum security

2. Increase awareness about cyberstalking in the society: awareness should be created through social media and messaging apps like WhatsApp, create awareness among users about how to protect themselves from cyberstalking

3. Careful sharing of personal information online: keep track of the information shared

4. Careful passwords management: change passwords often and regularly, keep strong passwords (include special characters and alternate use of upper and lower case letters and also include numbers. The longer the password, the longer it takes hackers to penetrate the system.

5. Enhancing privacy through configuration of privacy and security settings: check the privacy and security setting in any social site so as to reduce the case of anonymous stalking

6. Increase awareness about people accessing your profile: knowing who is accessing your profile helps one keep a track of such crimes, do not accept requests from random people on social networking websites, do not accept requests from random people on social networking websites; some can be hackers, some can be people following you offline with fake profiles online, be aware that people can create fake profiles and access our accounts, be aware that even friends and relatives may stake you

7. Responsible authorities need to take actions against the stalkers: cyber cell has to keep a track of stalkers to the extent possible, take complaints lodged to stalkers seriously and take strict actions against the stalkers (this can create a fear in the near future in the minds of the stalkers), technology to track the stalker needs to be improved to properly investigate the registered cases, there should be a quick action taken against stalkers which will scare the future stalkers and hackers

8. Keep track of (store, keep) your chats and conversations online: make a backup of the chats and data transferred in case of harassing in future, use the features available in every websites to easily keep track of your online conversations

9. Be aware about people you communicate with: avoid communicating with strangers on social sites as far as possible, make your account private which is visible to only your friends, it is good if we know the person with whom we are sharing our information or talking to

10. Keep personal ID and social ID separate: keep a separate Email ID for social sites, email id for social sites should be different from your personal email id, keep different passwords

11. Use trusted websites: use the network of trusted internet service providers

12. Protect your account by logging out: remember to log out shared networks, log out from your account whenever you are done using it, avoid saving passwords at public cyber cafe

13. Report stalking to appropriate authorities: unwanted threats or messages should be reported to respective authorities

14. Managing spam and phishing mails: keep a track of the spam mails in the accounts and report or block them immediately, do not click on links from suspicious sources, do not accept any request from the unknown person since the profile can be completely fake

Table 1. Results of Male participants

<table>
<thead>
<tr>
<th>No</th>
<th>Issues (11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Maintain security in your system: use of good and updated security software, renew your antivirus, always use updated software which assures maximum security</td>
</tr>
<tr>
<td>2</td>
<td>Increase awareness about cyberstalking in the society: awareness should be created through social media and messaging apps like WhatsApp, create awareness among users about how to protect themselves from cyberstalking</td>
</tr>
<tr>
<td>3</td>
<td>Careful sharing of personal information online: keep track of the information shared</td>
</tr>
<tr>
<td>4</td>
<td>Careful passwords management: change passwords often and regularly, keep strong passwords (include special characters and alternate use of upper and lower case letters and also include numbers. The longer the password, the longer it takes hackers to penetrate the system.</td>
</tr>
<tr>
<td>5</td>
<td>Enhancing privacy through configuration of privacy and security settings: check the privacy and security setting in any social site so as to reduce the case of anonymous stalking</td>
</tr>
<tr>
<td>6</td>
<td>Increase awareness about people accessing your profile: knowing who is accessing your profile helps one keep a track of such crimes, do not accept requests from random people on social networking websites, do not accept requests from random people on social networking websites; some can be hackers, some can be people following you offline with fake profiles online, be aware that people can create fake profiles and access our accounts, be aware that even friends and relatives may stake you</td>
</tr>
<tr>
<td>7</td>
<td>Responsible authorities need to take actions against the stalkers: cyber cell has to keep a track of stalkers to the extent possible, take complaints lodged to stalkers seriously and take strict actions against the stalkers (this can create a fear in the near future in the minds of the stalkers), technology to track the stalker needs to be improved to properly investigate the registered cases, there should be a quick action taken against stalkers which will scare the future stalkers and hackers</td>
</tr>
<tr>
<td>8</td>
<td>Keep track of (store, keep) your chats and conversations online: make a backup of the chats and data transferred in case of harassing in future, use the features available in every websites to easily keep track of your online conversations</td>
</tr>
<tr>
<td>9</td>
<td>Be aware about people you communicate with: avoid communicating with strangers on social sites as far as possible, make your account private which is visible to only your friends, it is good if we know the person with whom we are sharing our information or talking to</td>
</tr>
<tr>
<td>10</td>
<td>Keep personal ID and social ID separate: keep a separate Email ID for social sites, email id for social sites should be different from your personal email id, keep different passwords</td>
</tr>
<tr>
<td>11</td>
<td>Use trusted websites: use the network of trusted internet service providers</td>
</tr>
<tr>
<td>12</td>
<td>Protect your account by logging out: remember to log out shared networks, log out from your account whenever you are done using it, avoid saving passwords at public cyber cafe</td>
</tr>
<tr>
<td>13</td>
<td>Report stalking to appropriate authorities: unwanted threats or messages should be reported to respective authorities</td>
</tr>
<tr>
<td>14</td>
<td>Managing spam and phishing mails: phishing mails are meant to steal data from the computer and hence should be deleted, do not respond to spam and phishing mails</td>
</tr>
</tbody>
</table>
Important Issues for Preventing Cyberstalking in India

Table 3. Results of female participants

Future Directions & Conclusion

The goal of this research is to explicate the primary issues for cyberstalking prevention amongst men and women in the Indian context. This is done in order to compare these issues to existing stalking and cyberstalking legislation, policy and prevention efforts in India to highlight possible deficiencies. Hence, the next phase of this research is to engage in a comparative study to assess current shortfalls based on the top issues presented by men and women in India today. Ultimately, the study will expand and validate its sample size and then engage a qualitative analysis of existing stalking and cyberstalking legislation, policy and prevention efforts in India. From these efforts it is believed that enhanced cyberstalking-specific policy and legislation can be developed that clearly addresses the needs of those affected by cyberstalking in India.

REFERENCES