

Eliciting Societal Values for Cyberstalking Policy Decisions

Completed Research Paper

Kane J. Smith

Virginia Commonwealth University
301 W. Main St., Richmond, VA 23284
smithkj6@vcu.edu

Gurpreet Dhillon

Virginia Commonwealth University
301 W. Main St., Richmond, VA 23284
gdhillon@vcu.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 so it can be managed in the context of cybersecurity. To do this the problem question is twofold: First, what objectives are important based on the values of the general public with regard to the prevention of cyberstalking. Second, what are the possible scenarios for the implementation of these objectives that organizations, governments and society at large can look to that will guide their decision making process. In this paper we utilize Keeney's (1990) public value forum to elicit public values which can form the basis for the decision making process in preventing cyberstalking so institutions and governments can allocate resources prudently.

Keywords: Cyberstalking, cyber security planning, values, strategic objectives, qualitative research

Introduction

The problem of stalking has been well recognized in the academic and practitioner literature. With the advent of newer technologies such as social media, however, a new threat has emerged. An increased reliance of individuals on cyber social contact has resulted in a corresponding increase in possibility of interpersonal intrusion, referred to as cyberstalking (McFarlane & Bocij 2005). This increase in cyberstalking results in harassment and victimization through the use of the internet and can even spill out into the non-cyber world. Institutions and government bodies have struggled to manage this new phenomenon due to a lack of understanding in the prevention of cyberstalking. Therefore, in order to solve a problem, it is essential to understand it from the perspective of those affected by it and implement solutions which address their concerns. The problem question is then twofold for this study: First, what objectives are important based on the values of the general public with regard to the prevention of cyberstalking. Second, what are the possible scenarios for the implementation of these objectives that organizations, governments and society at large can look to that will guide their decision making process. The goal of answering both questions should result in the creation of useful and effective policy aimed at the prevention of cyberstalking. In order to answer these questions we utilize Keeney's (1990; 1992; 1996) public value forum and value based objectives to determine the most important objectives as well as the most highly rated scenarios for their implementation based on perceptions of the general public. This will serve as the basis for institutional decision-making process when developing policy aimed at the prevention of cyberstalking.

The paper is organized as follows: In section one, the basis for the public value forum and the use of value-based objectives is introduced and explained. In section two the basic process and structure of a public value forum is discussed. In section three we describe the application of the public value forum in which a sample of 21 individuals provided value inputs to the cyberstalking prevention policy decision-making

process. The results of this value forum are described in section four. In section five we conclude with a discussion of the meaning and implications of the results on cyberstalking prevention and policy making as well as the next steps in the process for informing policy decision making in this problem context.

Public Values for Making Cyberstalking Prevention Policy Decisions

Incorporating public values into the policymaking decision process has long been an acceptable practice, where the public's opinion is intended to drive policy creation and implementation (Dhillon et al. 2016; Dhillon & Torkzadeh 2006; Keeney 1996, Keeney 2013; Keeney and Palley 2013; May et al. 2013; Witesman & Walters 2014). Public opinion is driven by the inherent values of the collective individuals and can be useful in creating policy that is not only effective, but also accepted by those affected through its implementation (Keeney 1996; Dhillon et al. 2016; Dhillon & Torkzadeh 2006). Due to these considerations, public values are an important consideration within policy decisions, and therefore need to be incorporated into the decision making process despite being a difficult task (Dhillon et al. 2016; Dhillon & Torkzadeh 2006; Keeney 1996; Witesman & Walters 2014). Cyberstalking is a relatively new concept and research is being conducted with respect to things such as the characteristics of cyberstalkers (Cupach & Spitzberg 1998, 2001; Spitzberg et al. 1998; Spitzberg & Rhea 1999; Spitzberg et al. 2001) as well as the legal elements that must be evaluated (Goodno, 2007; Hazelwood & Koon-Magnin 2013). No work to date, however, has been done to elicit public values regarding this phenomenon to inform policy decisions that aim to prevent its occurrence. While public values are important and can aid in making policy decisions, it is still unclear how policy makers should interpret public values for a specific policy context (Dhillon et al. 2016; Dhillon & Torkzadeh 2006; Keeney 1990; 1996; 2013). According to Keeney (Dhillon et al. 2016; Dhillon & Torkzadeh 2006; Keeney 1990; 1996; 2013) this includes things such as; how public values should be operationalized, what role the experts and their values should have, and how expert recommendations and value interpretations should be combined in policy making. Further it should be noted that these issues become more complex as the policy context increases in scope and the problem domain increases in complexity (Dhillon et al. 2016; Dhillon & Torkzadeh 2006; Keeney 1990; 1996; 2013). Therefore, several approaches exist which can shed light and help to clarify public values in complex policy problems such as surveys, indirect and direct value elicitation, focus groups and public involvement (Dhillon et al. 2016; Dhillon & Torkzadeh 2006; Keeney 1990; 1996; 2013; May et al. 2013). Table 1 illustrates the advantages and disadvantages of each method of eliciting public values.

Method of Value Solicitation	Advantages	Disadvantages
Survey	<ul style="list-style-type: none"> Obtain Values in form of priorities among objectives, opinions about alternatives & preferences among alternatives Non-Binding, but informative 	<ul style="list-style-type: none"> Hypothetical nature of questions Influence of survey designer Difficulty in designing, administering and interpreting
Indirect Elicitation of Public Values	<ul style="list-style-type: none"> No direct questioning necessary Values inferred from behavior in marketplace Can be applied outside of marketplace 	<ul style="list-style-type: none"> Some values may not have a market equivalent that can be observed Questions are often hypothetical Form of question can greatly influence outcome
Direct Elicitation of Public Values	<ul style="list-style-type: none"> Interaction with individuals to elicit preferences and tradeoffs Numerous methods exist for rating and weighting Can improve tough policy decision making process 	<ul style="list-style-type: none"> Cost intensive Time intensive Hypothetical nature of questions
Focus Groups	<ul style="list-style-type: none"> High amounts of relevant information is gathered Adaptable and flexible format 	<ul style="list-style-type: none"> Groups often small and unrepresentative Data is often anecdotal
Public Involvement	<ul style="list-style-type: none"> Similar to Focus group, but has the intention of solving a particular problem Goes beyond testing reactions 	<ul style="list-style-type: none"> Restricted to smaller problems Places possible constraints on decision making

Table 1. Public Value Elicitation Methods (based on Keeney 1990)

In this paper, a combination of Survey, focus group and direct value elicitation techniques are utilized in what is termed by Keeney (1990) as the “public value forum”. From this model, we examine various objectives and scenarios that can inform policy decision making by organizations and public officials (Dhillon & Torkzadeh 2006; Keeney 2013; Witesman & Walters 2014). With respect to the prevention of cyberstalking, this is done by using a multi-attribute utility-based tradeoff procedure to elicit value-relevant information from a focus group to arrive at preferences for policy alternatives (Dhillon & Torkzadeh 2006; Keeney 1988, 1990, 1996, 2013; Keeney and Gregory 2005). Initially interviews were conducted to determine values that then allowed for the creation of objectives and their attributes with respect to the prevention of cyberstalking (Dhillon & Torkzadeh 2006; Keeney 1988, 1992; Keeney and Gregory 2005). A ‘WITI test’ (*Why Is This Important* test based on Keeney 1992) was performed to identify the fundamental objectives for the prevention of cyberstalking. From this, scenarios were created to present multiple policy implementation options for evaluation by the public value forum. The purpose of this study was three fold; Via a public value forum, our goal was to elicit public values about (1) five fundamental objectives aimed at the prevention of cyberstalking, (2) four overall cyberstalking prevention scenarios, and (3) each individual’s preference for the application of each given implementation scenario.

The Public Value Forum Methodology

The public value forum exists as a meeting of members of the general public, special interest groups or organizations that can last one to two days and usually involves anywhere between five and 25 participants (Keeney 1990; Keeney 2013). To begin, a policy problem is outlined, then the fundamental objectives relating to the problem are presented along with their particular attributes, and an objective value tree is created. ‘Good’ and ‘bad’ scenarios are created along with varying alternatives which can be presented to the value forum and discussed to find a preferable solution to the given policy problem (Keeney 1990, 1996, 2013). The next step is to identify and select members from the general public to participate in the study to which Keeney (1990) notes that there are two basic approaches to do so. The first approach is that of the stakeholder approach where groups who have a specific stake in the outcome of any policy decisions are identified and asked to participate in the study. This can be especially useful when covering a controversial topic due to the emphasis on negotiation and conflict resolution (Keeney 1990, 1996, 2013). The second way for selecting study participants for a value forum is the representative approach where members of the public are selected at random which is most useful when little to no knowledge exists about reasonable public values to drive policy decisions (Keeney 1990, 1996, 2013). Due to the relatively new nature of the cyberstalking phenomenon, little knowledge currently exists with respect to public values regarding policy decisions, and therefore the representative approach was selected for use in this study. Next, the Objectives and Attributes are defined and appropriate contrasting scenarios are created that illustrate ‘good’ and ‘bad’ scenarios as well as four alternatives of possible implementations of the defined objectives. Lastly, the value forum is conducted to elicit public values regarding cyberstalking prevention for policy decision-making and the results are analyzed.

The general structure of the value forum is (Keeney 1990):

1. The policy problem is introduced and participants motivated
2. Objectives and attributes are defined and clarified
3. Ranking and Single-attribute utility functions elicited from participants
4. Tradeoffs among the attributes are elicited from participants

The following is based on Keeney’s (1990) work and describes what each step of the value forum is intended to accomplish:

1. Introduction and Motivation. To begin the forum it is important to provide participants with an understanding of the importance of using public value judgments in their decision making process. Participants are given an opportunity to ask any questions regarding clarification of the topic, in this study cyberstalking, before moving on to stage 2.

2. Defining Objectives and Attributes. Participants are given the value tree and each objective with their corresponding attributes clarified. The scenarios are also presented and clarified answering any questions by participants before moving to stage 3.

3. Ranking and Elicitation of Single-Attribute Utility Functions. In stage 3 the quantitative levels of the attributes elicited may not be appropriate reflections of their relative desirability or utility. Therefore, utility functions are also used to demonstrate the relative desirability of a given objective or scenario. The choice of method depends on the purpose of the value forum and in many instances a simple rating method is sufficient.

4. Elicitation of Tradeoffs. Tradeoffs among attributes express the relative importance of attribute units by defining the exchange rate of one attribute unit vs. another. There are many methods for eliciting tradeoffs and relative importance information, such as swing weighting, and the choice of the appropriate method depends again on the policy context and the purpose of the value forum.

The Cyberstalking Prevention Value Forum

Prior to beginning the value forum, participants (N=21) were selected as a random sample of volunteers. The participants ranged in age from 22 to 55 and had a split of a few more women than men. Some participants had an educational background in Information Security while others had no previous experience or education in this area. Several of the participants had either been previous victims of cyberstalking or knew of friends and family who had been victimized. Participants were mostly US-born citizens, however several participants were non-US citizens, but as a group were representative of the demographics of any major metropolitan city of the mid-Atlantic region in the US. All participants were at least aware of the concept of cyberstalking prior to beginning the public value forum. After participants were selected, they were first asked to provide values regarding the prevention of cyberstalking. From these values, five objectives were created with defining attributes and the problem context was re-clarified to ensure the objectives addressed the values that were elicited from the participants. The values were elicited through personal interviews using suitable probing techniques that asked four open-ended questions regarding personal values towards the act of cyberstalking, created using Keeney's (1992) Value-Focused Thinking technique. These fundamental objectives were derived from the collective interviews using Keeney's (1992) 'WITT' test and presented to and discussed by the participants of the value forum. After the participants were satisfied with the fundamental objectives created by the value forum they were placed in the form of a value tree (see Figure 1). Any additional clarification or revision of the fundamental objectives was done at this time before moving to step 2 in the process.

Using these fundamental objectives, 'good' and 'bad' scenarios were created along with four alternate scenarios that represented differing instantiations of the five objectives based on the understanding of 'good' and 'bad' in the decision context. Once this was complete, a diagram (see Figure 1) representing the five objectives with their attributes, a 'value quote' and sub-objectives was developed and provided to the participants for reference during the remainder of the value forum. After this step of the value forum was completed, participants were given the task of providing objective ranking and weighting, both prior to reviewing the explanations of the objective meanings and then again at the end of the study. The participants were asked to rank the five objectives for the prevention of cyberstalking (See Table 2); first in order of their perceived importance (1 = Highest, 5 = Lowest), then they were asked to review the 'good' and 'bad' scenario for each objective and rank the magnitude of change or 'swing' between these scenarios for each objective from largest (1) to smallest (5). This means participants assigned a weight that indicated the relative magnitude of a given 'swing' with respect to the scenario they rated as having the largest degree of change between the 'good' and 'bad' scenario. From there, the objective rated 1 is then assigned a weight of 100, the lowest rating of 5 is given a weight of 0, and all others receive weight between 0-100 in decreasing increments by order of rank (Keeney 1990; Kirkwood, 1997). The purpose of the initial and final ranking and weighting was to determine how, if at all, the perceptions of participants change during the study from their initial impression. Initially they are only provided operational definitions of the objectives for the prevention of cyberstalking, but by the end of the study they have thoroughly examined a multitude of scenarios that express the potential applications of these objectives in real-world scenarios (Keeney 1990; Kirkwood 1997).

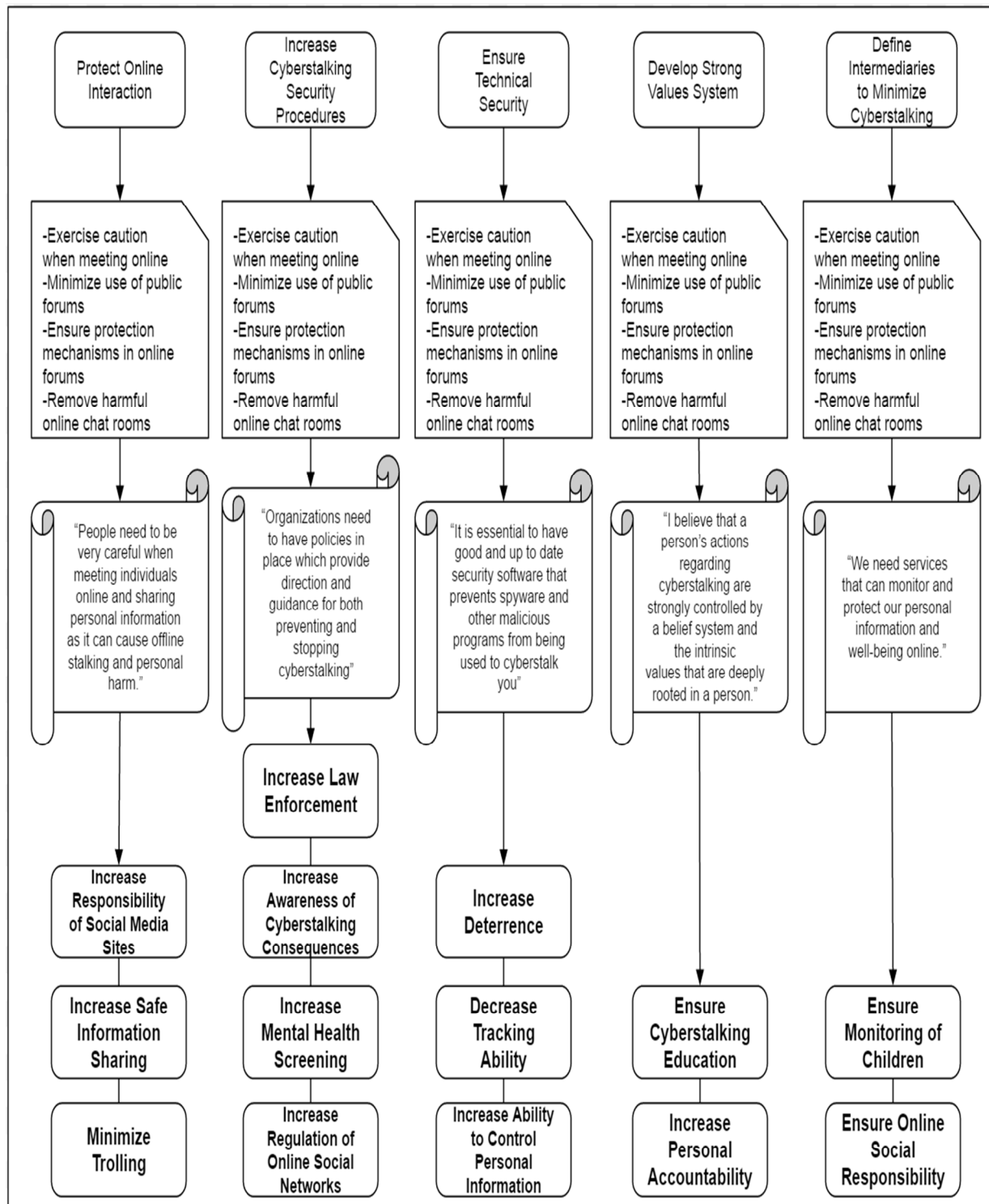


Figure 1. Objective Based Value Tree

<u>Objective Importance Swing % (0-100)</u>	<u>Objective Importance Swing Rank (1-5)</u>	<u>Objective Importance Rank (1-5)</u>	<u>Cyberstalking Fundamental Objectives</u>
90	2	1	Protect Online Interaction
80	3	2	Increase cyberstalking security procedures
100	1	3	Ensure technical security
0	5	5	Develop strong values system
60	4	4	Define intermediaries to minimize cyberstalking

Table 2. Example of Objective Ranking and Weighting

In addition to the ranking and weighting of the objectives, participants also examined scenarios labeled A, B, C and D which expressed different potential real-world instantiations of the cyberstalking prevention objective. These scenarios (see Table 3) were juxtaposed with the ‘good’ and ‘bad’ scenarios and participants were asked to rank them in order of preference with respect to the ‘good’ and ‘bad’ scenarios, with their most preferred scenario receiving a 2 and least preferred receiving a 5. The ‘good’ scenario was rated as 1 and bad as 6 in order to provide a conceptual basis of understanding in providing scenario preference ranks by the participants. After the ranking of the four scenarios, participants were asked to give an importance weight (Keeney 1990; Kirkwood 1997), again with respect to the ‘good’ and ‘bad’ scenarios, which were assigned 100 and 0 respectively. This was done to allow participants to demonstrate how close they felt the respective scenarios came to the conception of ‘good’ and ‘bad’ in these instantiations of the objectives beyond mere ranking (i.e. while a scenario may have ranked 2, a participant may have felt it was only 50% of the way to being a ‘good’ implementation of the objectives, so this allowed them to demonstrate how ‘close’ to good they felt a scenario came). Once this task of ranking the various scenarios was completed, participants were then asked to rank each instance of the scenarios A, B, C and D by the individual objective.

During the evaluation of the overall scenarios, participants may have been forced to select an overall scenario ranking based on only a few aspects of a given scenario which they assigned more importance to than one or more other parts (i.e. participants may have ranked scenario C as the most overall preferred but only felt one objective C scenario was most preferable). In order to determine if participants may have actually preferred a differing implementation of each objective by scenario, they were asked to rank each scenario individually by the objective (see Table 4). This allowed participants to, for example, select scenario C for the objective *Ensure Technical Security* as their most preferred while also being able to select scenario A for the objective *Increase Cyberstalking Security Procedures* as their most preferred. Participants were also asked to assign an importance weight to each ranking, using the same scale as before, with respect to how close to a ‘good’ implementation each scenario was represented. The purpose of this presented how preferred each individual scenario was to each participant and how relative to ‘good’ each scenario was as well. After the entire scenario ranking and weighting was accomplished the participants were finally asked to re-rank and weight the overall objectives for the prevention of cyberstalking as previously stated.

<u>Cyberstalking Fundamental Objectives</u>	<u>Good Scenario</u>	<u>Scenario A</u>	<u>Scenario B</u>	<u>Scenario C</u>	<u>Scenario D</u>	<u>Bad Scenario</u>
<u>PROTECT ONLINE INTERACTION</u>	<ul style="list-style-type: none"> -Highly secured and safe online meetings -Safe use of online public forums -Diverse protection mechanisms for online forums -Harmful online chat rooms eliminated 	<ul style="list-style-type: none"> -Online meeting sites highly regulated and can be removed by governments or organizations at will -Public online forums use must be approved beforehand -Protection mechanisms in online forums are mandatory -Online chat rooms considered harmful are removed entirely 	<ul style="list-style-type: none"> -Online meeting sites highly restricted and regulated, but allowed to exist -Use of public forums is highly regulated with some restrictions -Many protection mechanisms in online forums are mandatory, but not all -Online chat rooms considered harmful can be removed entirely 	<ul style="list-style-type: none"> -Online meeting sites regulated but users accept some risk in using them -Use of public forums has basic restrictions such as age or prior consent to use -Protection mechanisms in online forums are 'opt out' at the users discretion -Online chat rooms considered harmful are labeled harmful and have basic restrictions for viewing 	<ul style="list-style-type: none"> -Online meeting sites have little to no regulation, user assumes all risk -Public forums unregulated and unrestricted as users determine all content -Any protection mechanisms for an online forums are 'opt in' by user -Online chat rooms considered harmful allowed to exist with no warnings, users must avoid on their own 	<ul style="list-style-type: none"> -Online meetings are insecure with no regulation -Dangerous forums are allowed in any form to public -No protection mechanisms for online forums -Harmful online chat rooms run rampant
<u>INCREASE CYBERSTALKING SECURITY PROCEDURES</u>	<ul style="list-style-type: none"> -Secure online browsing -Strict user authentication measures -High availability of cyberstalking prevention tools -Websites validated for trustworthiness 	<ul style="list-style-type: none"> -All browsing security measure's use online enforced by law -Authentication measures compelled by law for all online use -Cyberstalking prevention tools required by law -All websites must be evaluated for trustworthiness and approved before posting to internet 	<ul style="list-style-type: none"> -Some browsing security measure's use online enforced by law -Some authentication measures compelled by law for all online use -Some cyberstalking prevention tools required by law -All websites evaluated for trustworthiness, but those that fail are clearly marked as untrustworthy by law 	<ul style="list-style-type: none"> -Browsing security measures online exist and are 'opt-out' by user -Authentication measures on my default for all online use, but user can 'opt-out' -Cyberstalking prevention tools exist by law but user can 'opt-out' of use -Websites can be evaluated for trustworthiness and labeled as such, but no requirement to label untrusted sites 	<ul style="list-style-type: none"> -Any browsing security measures are 'opt-in' by user and not required by law -Authentication measures exist but not required, user assumes all risk -Cyberstalking prevention tools disabled by default, user must 'opt-in' to use -All websites are not required to be evaluated for trustworthiness and are labeled at owner discretion 	<ul style="list-style-type: none"> -Insecure online browsing -No user authentication measures -No available cyberstalking prevention tools -Websites not validated for trustworthiness
<u>ENSURE TECHNICAL SECURITY</u>	<ul style="list-style-type: none"> -High investment in safe browsing technologies -All available tools used to prevent stealing of information online -Login credentials managed effectively -All security settings can be managed for online activity -Online filters can block negative behavior 	<ul style="list-style-type: none"> -Government mandated investment in safe browsing technologies by organizations -All available tools to prevent stealing of information required by law -Safe login credentials management regulated by government -Security settings online monitored and enforced by government or organizations -Online filters to block negative behavior compulsory 	<ul style="list-style-type: none"> -Some government mandated minimum investment in safe browsing technologies by organizations -Some minimum tools to prevent stealing of information required by law -Safe login credentials management required, but managed by organization and user -Some security settings online are compulsory -Some use of online filters to block negative behavior compulsory 	<ul style="list-style-type: none"> -Investment in safe browsing technologies controlled solely by organizations -Available tools to prevent stealing of information exist and are 'opt-out' by user -Safe login credentials management regulated by user and are 'opt-out' -Security settings online monitored and enforced by user and are 'opt-out' -Online filters to block negative behavior managed by user and are 'opt-out' 	<ul style="list-style-type: none"> -Limited investment in safe browsing technologies -Some tools to prevent stealing of information exist and are 'opt-in' by user -Safe login credentials management regulated by user and are 'opt-in' -Some security settings online can be monitored by user, but are 'opt-in' -Any online filters to block negative behavior are managed by user who must 'opt-in' 	<ul style="list-style-type: none"> -No investment in safe browsing technologies -No available tools to prevent stealing of information online -Login credentials not managed at all -No security settings for protecting online activity -No online filters to block negative behavior
<u>DEVELOP STRONG VALUES SYSTEM</u>	<ul style="list-style-type: none"> -Strong family values that prevent cyberstalking -Social pressures reduce or eliminate cyberstalking -Family support ensures safe information sharing measures 	<ul style="list-style-type: none"> -Mandatory programs to impart strong family values to deter cyberstalking -Intense social pressures to reduce cyberstalking supported by various programs -Family support mandatory in ensuring information protection measures by users 	<ul style="list-style-type: none"> -Programs exist to impart strong family values to deter cyberstalking with minimum attendance required -Some social pressures used to reduce cyberstalking supported by various programs -Family support encouraged in ensuring information protection measures by users 	<ul style="list-style-type: none"> -Some programs exist to impart strong family values to deter cyberstalking, people can 'opt-out' -Some social pressures encouraged to reduce cyberstalking -Minimum level of family support encouraged to ensuring information protection of users 	<ul style="list-style-type: none"> -Programs exist to impart strong family values to deter cyberstalking, but are 'opt-in' -Little social pressure to reduce cyberstalking -Little family support encouraged for ensuring information protection measures by users 	<ul style="list-style-type: none"> -Lack of family values encourages cyberstalking behavior -Social pressures encourage cyberstalking -No family support to ensure safe information sharing online
<u>DEFINE INTERMEDIARIES TO MINIMIZE CYBERSTALKING</u>	<ul style="list-style-type: none"> -Online payment systems ensure security -Services for hire protect consumer online information -Personal information insurance protects privacy -Trust forming mechanisms exist to protect against cyberstalking 	<ul style="list-style-type: none"> -Third party payment systems mandated and regulated to ensure online security -Services for hire mandated to protect consumer online information -Personal online information insurance required to protect privacy -Mandatory trust forming mechanisms to protect against cyberstalking 	<ul style="list-style-type: none"> -Third party payment systems exist to ensure online security with minimum use required -Services for hire exist to protect consumer online information with minimum use required -Personal online information insurance minimum required to protect privacy -Some mandatory trust forming mechanisms required to protect against cyberstalking 	<ul style="list-style-type: none"> -Third party payment systems exist to ensure online security, used at user discretion -Services for hire exist to protect consumer online information, used at user discretion -Personal online information insurance exist but not required to protect privacy -Some minimum mandatory trust forming mechanisms required to protect against cyberstalking 	<ul style="list-style-type: none"> -Few third party payment systems exist to ensure online security -Few services for hire to protect consumer online information -Personal online information insurance not required to protect privacy and has no regulation for coverage -No mandatory trust forming mechanisms to protect against cyberstalking 	<ul style="list-style-type: none"> -Online payment systems lack security -No services exist to protect consumer online information -No personal information insurance to protect privacy -No trust forming mechanisms exist to protect against cyberstalking
<u>Scenario Rank (1-6)</u>	1	5	3	2	4	6
<u>Scenario % (0-100)</u>	100	10	80	90	50	0

Table 3. Scenario Ranking

Scenarios	PROTECT ONLINE INTERACTION	Rank (1-6)	Weight (0-100)	INCREASE CYBERSTALKING SECURITY PROCEDURES	Rank (1-6)	Weight (0-100)	ENSURE TECHNICAL SECURITY	Rank (1-6)	Weight (0-100)	DEVELOP STRONG VALUES SYSTEM	Rank (1-6)	Weight (0-100)	DEFINE INTERMEDIARIES TO MINIMIZE CYBERSTALKING	Rank (1-6)	Weight (0-100)
Good Scenario	<ul style="list-style-type: none"> -Highly secured and safe online meetings -Safe use of online public forums -Diverse protection mechanisms for online forums -Harmful online chat rooms eliminated 	1	100	<ul style="list-style-type: none"> -Secure online browsing -Strict user authentication measures -High availability of cyberstalking prevention tools -Websites validated for trustworthiness 	1	100	<ul style="list-style-type: none"> -High investment in safe browsing technologies -All available tools used to prevent stealing of information online -Login credentials managed effectively -All security settings can be managed for online activity -Online filters can block negative behavior 	1	100	<ul style="list-style-type: none"> -Strong family values that prevent cyberstalking -Social pressures reduce or eliminate cyberstalking -Family support ensures safe information sharing measures 	1	100	<ul style="list-style-type: none"> -Online payment systems ensure security -Services for hire protect consumer online information -Personal information insurance protects privacy -Trust forming mechanisms exist to protect against cyberstalking 	1	100
Scenario A	<ul style="list-style-type: none"> -Online meeting sites highly regulated and can be removed by governments or organizations at will -Public online forums use must be approved beforehand -Protection mechanisms in online forums are mandatory -Online chat rooms considered harmful are removed entirely 			<ul style="list-style-type: none"> -All browsing security measure's use online enforced by law -Authentication measures compelled by law for all online use -Cyberstalking prevention tools required by law -All websites must be evaluated for trustworthiness and approved before posting to internet 			<ul style="list-style-type: none"> -Government mandated investment in safe browsing technologies by organizations -All available tools to prevent stealing of information required by law -Safe login credentials management regulated by government -Security settings online monitored and enforced by government or organizations -Online filters to block negative behavior compulsory 			<ul style="list-style-type: none"> -Mandatory programs to impart strong family values to deter cyberstalking -Intense social pressures to reduce cyberstalking supported by various programs -Family support mandatory in ensuring information protection measures by users 			<ul style="list-style-type: none"> -Third party payment systems mandated and regulated to ensure online security -Services for hire mandated to protect consumer online information -Personal online information insurance required to protect privacy -Mandatory trust forming mechanisms to protect against cyberstalking 		
Scenario B	<ul style="list-style-type: none"> -Online meeting sites highly restricted and regulated, but allowed to exist -Use of public forums is highly regulated with some restrictions -Many protection mechanisms in online forums are mandatory, but not all -Online chat rooms considered harmful can be removed entirely 			<ul style="list-style-type: none"> -Some browsing security measure's use online enforced by law -Some authentication measures compelled by law for all online use -Some cyberstalking prevention tools required by law -All websites evaluated for trustworthiness, but those that fail are clearly marked as untrustworthy by law 			<ul style="list-style-type: none"> -Some government mandated minimum investment in safe browsing technologies by organizations -Some minimum tools to prevent stealing of information required by law -Safe login credentials management required, but managed by organization and user -Some security settings online are compulsory -Some use of online filters to block negative behavior compulsory 			<ul style="list-style-type: none"> -Programs exist to impart strong family values to deter cyberstalking with minimum attendance required -Some social pressures used to reduce cyberstalking supported by various programs -Family support encouraged in ensuring information protection measures by users 			<ul style="list-style-type: none"> -Third party payment systems exist to ensure online security with minimum use required -Services for hire exist to protect consumer online information with minimum use required -Personal online information insurance minimum required to protect privacy -Some mandatory trust forming mechanisms required to protect against cyberstalking 		
Scenario C	<ul style="list-style-type: none"> -Online meeting sites regulated but users accept some risk in using them -Use of public forums has basic restrictions such as age or prior consent to use -Protection mechanisms in online forums are 'opt out' at the users discretion -Online chat rooms considered harmful are labeled harmful and have basic restrictions for viewing 			<ul style="list-style-type: none"> -Browsing security measures online exist and are 'opt-out' by user -Authentication measures on my default for all online use, but user can 'opt-out' -Cyberstalking prevention tools exist by law but user can 'opt-out' of use -Websites can be evaluated for trustworthiness and labeled as such, but no requirement to label untrusted sites 			<ul style="list-style-type: none"> -Investment in safe browsing technologies controlled solely by organizations -Available tools to prevent stealing of information exist and are 'opt-out' by user -Safe login credentials management regulated by user and are 'opt-out' -Security settings online monitored and enforced by user and are 'opt-out' -Online filters to block negative behavior managed by user and are 'opt-out' 			<ul style="list-style-type: none"> -Some programs exist to impart strong family values to deter cyberstalking, people can 'opt-out' -Some social pressures encouraged to reduce cyberstalking -Minimum level of family support encouraged to ensuring information protection of users 			<ul style="list-style-type: none"> -Third party payment systems exist to ensure online security, used at user discretion -Services for hire exist to protect consumer online information, used at user discretion -Personal online information insurance exist but not required to protect privacy -Some minimum mandatory trust forming mechanisms required to protect against cyberstalking 		
Scenario D	<ul style="list-style-type: none"> -Online meeting sites have little to no regulation, user assumes all risk -Public forums unregulated and unrestricted as users determine all content -Any protection mechanisms for an online forums are 'opt in' by user -Online chat rooms considered harmful allowed to exist with no warnings, users must avoid on their own 			<ul style="list-style-type: none"> -Any browsing security measures are 'opt-in' by user and not required by law -Authentication measures exist but not required, user assumes all risk -Cyberstalking prevention tools disabled by default, user must 'opt-in' to use -All websites are not required to be evaluated for trustworthiness and are labeled at owner discretion 			<ul style="list-style-type: none"> -Limited investment in safe browsing technologies -Some tools to prevent stealing of information exist and are 'opt-in' by user -Safe login credentials management regulated by user and are 'opt-in' -Some security settings online can be monitored by user, but are 'opt-in' -Any online filters to block negative behavior are managed by user who must 'opt-in' 			<ul style="list-style-type: none"> -Programs exist to impart strong family values to deter cyberstalking, but are 'opt-in' -Little social pressure to reduce cyberstalking -Little family support encouraged for ensuring information protection measures by users 			<ul style="list-style-type: none"> -Few third party payment systems exist to ensure online security -Few services for hire to protect consumer online information -Personal online information insurance not required to protect privacy and has no regulation for coverage -No mandatory trust forming mechanisms to protect against cyberstalking 		
Bad Scenario	<ul style="list-style-type: none"> -Online meetings are insecure with no regulation -Dangerous forums are allowed in any form to public -No protection mechanisms for online forums -Harmful online chat rooms run rampant 	6	0	<ul style="list-style-type: none"> -Insecure online browsing -No user authentication measures -No available cyberstalking prevention tools -Websites not validated for trustworthiness 	6	0	<ul style="list-style-type: none"> -No investment in safe browsing technologies -No available tools to prevent stealing of information online -Login credentials not managed at all -No security settings for protecting online activity -No online filters to block negative behavior 	6	0	<ul style="list-style-type: none"> -Lack of family values encourages cyberstalking behavior -Social pressures encourage cyberstalking -No family support to ensure safe information sharing online 	6	0	<ul style="list-style-type: none"> -Online payment systems lack security -No services exist to protect consumer online information -No personal information insurance to protect privacy -No trust forming mechanisms exist to protect against cyberstalking 	6	0
Objective Rank (1-5)															
Objective Swing Rank (1-5)															
Objective Swing Weighting (0-100)															

Table 4. Individual Scenario Ranking Survey

Results of the Public Value Forum

With the data collection from participants completed, an analysis was conducted on the findings for which the results will be discussed in the following three parts; First, the overall initial and final Importance and Swing rankings and Swing weightings. Second, the overall scenario ranking and weightings and lastly, the individual scenario ranking and weightings by objective.

Initial Importance Rank, Swing rank and Swing weight Data

To begin, each of the five objectives were defined for the participants and they were asked to rank them in order of importance (See Table 5). The study found that in the initial rankings of the objectives, participants provided *Ensure Technical Security* (ETS) and *Increase Cyberstalking Security Procedures* (ICSP) with the highest overall median ranks of 2, while the objective *Protect Online interaction* (POI) was assigned a median rank of 3 and *Develop Strong Values System* (DSVS) and *Define Intermediaries to Prevent Cyberstalking* (DIPC) were assigned median rankings of 4. Based on these initial rankings, participants, with only a definitional understanding of the objectives, clearly rate technical and procedural prevention measures highest in importance in the prevention of cyberstalking.

Next, participants assigned swing ratings for each objective based on the ‘good’ and ‘bad’ scenarios provided, which revealed that the difference between ‘good’ and ‘bad’ scenarios for each objective were like-wise rated highest in the technical and procedural objectives with ETS and ICSP each receiving a median swing rank of 2. Interestingly, it was found that participants also found DIPC had a large change from ‘bad’ to good’ and provided a median rank of 3, while POI and DSVS were given median ranks of 4. This seems to indicate that participant’s felt that not only were ETS and ICSP very important overall, the swing between ‘good’ and ‘bad’ implementations was likewise the largest contrast. With the weights (Keeney 1990; Kirkwood 1997) for each swing ranking, participants were asked to demonstrate how drastic the change between ‘good’ and ‘bad’ scenarios was for each objective. This provided an astounding result that demonstrated how important the objectives were as ETS and ICSP received mean weights of 83.19 and 74.33 respectively (out of 100), while DIPC received 65.05, POI 56.95 and DSVS a mere 40.62 mean weight. This would lead one to conclude that if faced with limited resources a strong focus on technical and procedural prevention objectives might address the most pressing concerns of engaged users as these objectives were not only rated the highest, but also weighted most heavily by participants as having the largest degree of impact between a ‘bad’ and ‘good’ implementation.

Objective	Median of Importance Rank	Median Rank of Swing Weights	Mean of Swing Weights
Protect Online Interaction	3	4	56.95
Increase Cyberstalking Security Procedures	2	2	74.33
Ensure Technical Security	2	2	83.19
Develop Strong Values System	4	4	40.61
Define Intermediaries to Prevent Cyberstalking	4	3	65.04

Table 5. Initial Ranking and Weighting Results

Final Importance Rank, Swing rank and Swing weight Data

After the overall and individual scenario ranking and weighting was completed, participants were then asked to re-evaluate their prior objective ranking and weightings to determine whether after seeing potential real-world implementations of the objectives their perceptions towards them had changed (See Table 6). It was found that the overall importance rankings stayed relatively similar, with ETS and ICSP retaining median rankings of 2; however POI rose in its median ranking to 2 from 3, while DSVS and DIPC stayed the same with a median ranking of 4 for each. Swing rankings for each objective changed the most dramatically as it appears that seeing proposed instances of implementation enhanced participants understanding of the objectives. Median swing ranks for ETS and ICSP remained at 2, while POI moved up from 4 to 3, DIPC stayed at 3 and DSVS fell from 4 to 5. To highlight the magnitude of these changes, POI initially had a mean weight of 56.95 its mean weight on the final evaluation rose to 72.67, while the fall of DSVS from 4 to 5 in swing rank did not result in such a large change (40.62 to 40.24 mean weight). DIPC saw a large drop in mean weight from 65.05 to 52.19 even though it retained the swing rank of 3.

Objective	Median of Importance Rank	Mean of Swing Weights	Median Rank of Swing Weights
Protect Online Interaction	2	72.66	3
Increase Cyberstalking Security Procedures	2	76.9	2
Ensure Technical Security	2	80.00	2
Develop Strong Values System	4	40.23	5
Define Intermediaries to Prevent Cyberstalking	4	52.19	3

Table 6. Final Ranking and Weighting Results

This final recap of Importance Rank, Swing Rank and Swing Weight is useful because it re-emphasizes the importance of the technical and procedural objectives as well as highlights the impact ‘good’ and ‘bad’ implementations of each objective has in the public perception of the prevention of cyberstalking. Further, a deeper understanding of POI revealed that when participants were provided with real-world examples of scenarios illustrating the objectives, the protection of their online interactions received more importance and the difference between ‘good’ and ‘bad’ scenarios was viewed as much greater than they initially perceived. This finding revealed the importance of both creating a comprehensive understanding of the concept of the cyberstalking prevention objectives as well as how real-world instantiations of each objective can impact the public’s conceptions of an objective’s importance with respect to ‘good’ and ‘bad’ implementations.

Scenario Selection Preference

As an organization that is looking to prevent and protect customers from cyberstalking, understanding the importance of the objective to their users is useful in directing the allocation of finite resources. It is also of equal importance, however, to understand the means by which a government organization can enact those objectives to prevent cyberstalking and prior to doing so, anticipate the preferred method by which users will respond to those measures in the most positive way. This was first done in the study by having participants evaluate the scenario ‘options’ in a holistic manner where the scenarios, labeled A, B, C and D, ranged from high organization involvement (scenario A) to very little organization involvement (scenario D). Participants were asked to rank, based on their preference, the order in which the scenarios represented ‘good’ to ‘bad’ options, with 2 being their most preferred and 5 being their least preferred

overall scenario for the objective's implementation. Lastly, participants weighted their rankings relative to how 'good' or 'bad' they were compared to the baseline good and bad scenarios.

The results from this portion of the study (see Table 7) provided insight into the consumer preferences with respect to the actions a government body or organization should take in the prevention of cyberstalking. The study found that participants heavily favored scenario C with a median rank of 2 and a mean weight of 79.19, demonstrating that they found an option where the technical tools and procedures exist and can be turned on or off at the preference of the user and that some level of regulation is preferred in order to ensure the adequacy of these prevention methods. By contrast, scenario D was the least preferred of all the scenarios receiving a median rank of 5 and a mean weight of 45.19, indicating that participants did not find a 'hands off' approach appealing. This approach leaves the vast majority of the responsibility for prevention in the hands of the user. This contrast is very important for government organizations as it demonstrates that users clearly want mechanisms in place that work to prevent cyberstalking, but they prefer to maintain a level of control and discretion over the exact use and implementation of those prevention mechanisms as opposed to having mechanisms forced upon them.

Scenario	Median Rank	Mean Weight
A	3	59.76
B	3	65.81
C	2	78.19
D	5	45.19
Good	1	100
Bad	6	0

Table 7. Overall Scenario Ranking and Weighting Results

Individual Scenario selection by Objective

In this final portion of the study participants were asked to rank, in order of preference, each scenario by the objective. This was done to assess whether participants may prefer different methods of cyberstalking prevention implementation based on the given objective. The results (see Table 8) from this method of individual scenario selection and preference indicate that, generally scenario B and C, are the preferred choices for objective implementation with scenario B leading scenario C in every objective but POI. This is interesting to note as scenario B in POI calls for a high degree of mandatory regulation which could have caused participants who would likely have preferred scenario B overall to instead select the less restrictive scenario C and rank it higher in a holistic situation. However, individually, scenario B is generally more preferred than scenario C, but are clearly the two most preferred scenarios overall for the cyberstalking prevention objectives. This is still in line with the original inference from the previous section where it appears participants still prefer a degree of autonomy in the final implementation of these objectives, but like-wise want a degree of regulation and law to enforce the existence of procedures, guidelines and technical controls. Based on these results it would be reasonable to suggest that users would prefer an 'opt-out' method where the existence of cyberstalking prevention tools were enforced in law, but the ultimate use by consumers was at their own discretion.

	PROTECT ONLINE INTERACTION		INCREASE CYBERSTALKING SECURITY PROCEDURES		ENSURE TECHNICAL SECURITY		DEVELOP STRONG VALUES SYSTEM		DEFINE INTERMEDIARIES TO MINIMIZE CYBERSTALKING	
Scenarios	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)
Good Scenario	1	100	1	100	1	100	1	100	1	100
Scenario A	4	67.05	3	70.57	3	74.90	4	63.24	3	71.38
Scenario B	3	71.90	3	77.29	3	75.52	2	75.38	3	72.43
Scenario C	3	77.67	3	70.62	3	70.48	4	66.67	4	67
Scenario D	5	37.52	5	40.71	5	43.62	5	43.86	5	46.24
Bad Scenario	6	0	6	0	6	0	6	0	6	0

Table 8. Individual Scenario Ranking and Weighting Results

Discussion

After reviewing the results and drawing on the insights of each individual section herein, three distinct broad conclusions can be drawn based on this research. The first is that baseline regulations must exist in order to aid organizations in the prevention of cyberstalking and provide users with the confidence that the issue is being addressed. The second is that users desire technical controls in place that can be used to protect them and their information from potential cyberstalking. Finally, while albeit related to the previous two, users want the freedom to choose to what extent the regulations and controls for prevention of cyber stalking should be implemented. These three distinct conclusions provide a great deal of insight into the values of the general public regarding the prevention of cyberstalking at an organizational level. The results of the public value forum demonstrate a clear desire by participants to have clear regulations, policies and procedures that elucidate required protections against cyberstalking. Scenario D that provided little or no governance to this issue, regardless of objective, was the least preferred by virtually all participants, as it received no top rankings and 12 last place rankings. Participants additionally demonstrated this need for strong technical controls both by ranking Ensure Technical Security highly in the objective ratings as well as through the selection of scenarios, which indicated a high degree of technical tools, which would be available to users for protection from cyberstalking. In the application of policy and technical controls, participants demonstrated clear preferences for control over final implementation and enforcement. By reviewing the scenario selection and individual scenario preferences it was shown that participants still prefer a degree of control, which would likely aid in the successful implementation of policy.

At a scenario level, Scenario C was the clear preference in the value forum, which was composed of individual instantiations of the five objectives for preventing cyberstalking and had the following characteristics: Some general government mandated regulations about policy and technical controls, a bevy of technical control options available to the user and the ability of users to 'opt-out' from these controls if they felt it added undue burden or restriction. This is important to note in the context of the overall user scenario selection. It can be said that even if something is 'good for you,' if it is forced upon the user, they may reject it regardless of the risk, for which there is some support in the literature for this assertion. As Herley (2009), in the context of security and usability noted, "users reject advice since it offers to shield them from the direct costs of attacks, but burdens them with increased indirect costs, or externalities. Since the direct costs are generally small relative to the indirect ones they reject this bargain. Since victimization is rare, and imposes a one-time cost, while security advice applies to everyone and is an ongoing cost, the burden ends up being larger than that caused by the ill it addresses." Having some regulation to enforce protocols and technical controls in place, but giving the user freedom in choosing

the level of restriction proved popular even at the individual scenario ranking level where scenario B options tended to be the most preferred with C a close second overall. Scenario B tended to provide similar options to C, but the difference was that when it comes to procedures and technical controls, users clearly feel it is better to have procedures and technical controls clearly defined by the law. These points clearly support the three distinct conclusions drawn and mentioned previously in that they illustrate a very clear desire among the general public to have well defined laws, regulations, procedures and technical controls for the prevention of cyberstalking. This leads us to the limitations of the current study as well as the future directions of this cyberstalking prevention research stream.

The current limitation of this study is that it did not include Keeney's (Keeney 1990, 2013; Dhillon & Torkzadeh 2006; May et al. 2013) fifth step of constructing a multi-attribute utility model and the evaluation of alternatives through the use of an expert panel. In the construction of a multi-attribute utility model the tradeoff information elicited in step 4 is converted into weights for the attributes using standard multi-attribute utility techniques (Dhillon & Torkzadeh 2006; Keeney 1990). In the vast majority of instances the multi-attribute utility model in question is a simple weighted average of the single-attribute utilities; some can be more complex multiplicative or multilinear models (Dhillon & Torkzadeh 2006; Keeney 1990, 2013). In the case of this research, it is believed that a more complex model needs to be chosen and therefore additional tradeoff questions will need to be asked that will elicit additional parameters for a model (Dhillon & Torkzadeh 2006; Keeney 1990, 2013). To do this, a multi-attribute utility model is created from a combination of expert assessments of the single-attribute performance of the scenario alternatives to generate an overall evaluation (Dhillon & Torkzadeh 2006; Keeney 1990, 2013). This is to say that, the expert opinions not present in this study (a current limitation) will be elicited from a panel of industry experts and then additively placed in a model along with the results of the general public's value forum. This will create a model that demonstrates both the values of the general public as well as the values of industry experts and will serve as the next step in the direction of this research. In a future research a panel of 5 industry experts ranging from a CIO to an attorney specializing in cyberstalking and stalking legal matters will be engaged in an 'expert' value forum that will elicit their values for use in the creation of a multi-attribute utility model. This new model will then serve as the foundation for additional research to establish a clear methodology for the decision making process to create and implement policies intended to prevent cyberstalking.

Conclusion

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 and the public value forum, revealed the objectives and scenarios which the general public find most important and provide the greatest perceived deterrent to cyberstalking, which are essential for developing measures and protections against cyberstalking at a policy level by governments and organizations. Therefore, this is a significant contribution as previous research in this area is under-developed and as such falls short of being able to propose tangible measures and protections against cyberstalking. Results clearly indicate a strong preference by the general public for technical and procedural controls aimed at the prevention of cyberstalking at a policy level, but still leaves final control over the exact implementation to the people themselves. The next steps in this research will extend the process further and provide a multi-attribute utility model that will incorporate the values of cyberstalking experts in order to provide an exact model for the creation of cyberstalking prevention policy at a governmental and organizational level.

References

- Cupach, W. and Spitzberg, B. 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.
- Cupach, W. and Spitzberg, B. 2001. 'Obsessive Relational Intrusion: Incidence, Perceived Severity, and Coping', *Violence and Victims* 15(1): 1–16.
- Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. *Computers in Human Behavior*, 61, 656–666.

- Dhillon, G., & Torkzadeh, G. 2006. Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16(3), 293-314.
- Goodno, N. H. 2007. Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws; *Missouri Law Review*, Vol 72, Issue 1.
- Hazelwood, S., & Koon-Magnin, S. 2013. Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis. *International Journal of Cyber Criminology*, 7(2), 155-168.
- Herley, C. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 133-144). ACM.
- Keeney, R. L. 1988. Structuring objectives for problems of public interest. *Operations Research* 36(3), 396-405.
- Keeney, R. L., Winterfeldt, D. V., & Eppel, T. 1990. Eliciting Public Values for Complex Policy Decisions. *Management Science*, 36(9), 1011-1030.
- Keeney, R. L. 1992. Value-Focused Thinking: A Path to Creative Decision making. Harvard University Press.
- Keeney, R. L. 1996. Value-focused thinking: Identifying decision opportunities and creating alternatives. *European Journal of Operational Research* 92(3), 537-549.
- Keeney, R. L. and Gregory R. S. 2005. Selecting attributes to measure the achievement of objectives. *Operations Research* 53(1), 1-11.
- Keeney, R. L. 2013. Foundations for Group Decision Analysis. *Decision Analysis*, 10(2), 103-120.
- Keeney, R. L., & Palley, A. B. 2013. Decision Strategies to Reduce Teenage and Young Adult Deaths in the United States. *Risk Analysis*, 33(9), 1661-1676.
- Kirkwood, C. W. 1997. Strategic Decision Making, Multi-objective Decision Analysis with Spreadsheets. Belmont: Wadsworth Publishing Company.
- May, J., Dhillon G., and Caldeira M. 2013. Defining value-based objectives for ERP systems planning. *Decision Support Systems* 55(1), 98-109.
- McFarlane, L., & Bocij, P. 2005. An exploration of predatory behavior in cyberspace: Towards a typology of cyber stalkers. Retrieved Feb 18, 2016, from http://firstmonday.org/issues/issues8_9/mcfarlane/index.html.
- Spitzberg, B., Nicastro, A. & Cousins, A. 1998. 'Exploring the Interactional Phenomenon of Stalking and Obsessive Relational Intrusion', *Communication Reports* 11(1): 33-48.
- Spitzberg, B. & Rhea, J. 1999. 'Obsessive Relational Intrusion and Sexual Coercion Victimization', *Journal of Interpersonal Violence* 14(1): 3-20.
- Spitzberg, B., Marshall, L. & Cupach, W. 2001. 'Obsessive Relational Intrusion, Coping, and Sexual Coercion Victimization', *Communication Reports* 14(1): 19-30.
- Witesman, E. M., & Walters, L. C. 2014. Modeling Public Decision Preferences Using Context-Specific Value Hierarchies. *The American Review of Public Administration*, 45(1), 86-105.