Australian Internet Users and Guardianship against Cyber Abuse: An Empirical Analysis

Zarina I. Vakhitova[1] **& Danielle M. Reynald**[2]
Griffith University, Australia

Abstract

This study presents an empirical analysis of guardianship against abuse in cyberspace. Building upon the existing body of knowledge about active guardianship processes in the physical world, this study extends our understanding of how these processes operate in the unique setting of cyberspace. To collect information about cyber guardians and cyber abuse events witnessed by the guardians, an online survey of adult Australian users of the Internet and social media sites was conducted (n = 650). The results show that contextual awareness of cyberspace was predictive of witnessing and intervening in the events of cyber abuse. Based on the empirical results, the study makes practical recommendations on how crime prevention efforts could be boosted in cyberspace.

Keywords: contextual awareness, cyberspace, cyber abuse, cyber guardianship.

Introduction

Cyberspace has made it easier to communicate, to learn, and to do business with people from all over the world. It has also made it easier for stalkers and harassers to select and target their victims. Similar to real-world stalking and harassment, cyber abuse can cause victims psychological and emotional harm, and, in extreme cases, can lead to suicide (Bocij, 2004; Finn, 2004). Although cyber abuse (which includes cyber stalking and cyber harassment) is a very recent phenomenon, it is becoming a serious problem. A U.S. study showed that as high as 30% of college students could be victims of cyber abuse (Reyns et al., 2012). What is even more alarming is that rates of cyber abuse, at least among the youth, appear to be on the rise in many countries, including the United States, Canada, Turkey, Hong Kong, and Taiwan (Hinduja & Patchin, 2009; Jones et al., 2012; Beran & Li, 2005, 2007; Erdur-Baker, 2010; Hokoda et al., 2006; Wong et al., 2008). As more people get connected to the Internet and participate in social networking activities, more Internet users will be exposed to the risks associated with cyberspace activities. The likely increase in incidents of cyber abuse, coupled with potentially serious consequences to the victims, point to the importance of finding a solution to this emerging problem.

[1]Doctoral Candidate, School of Criminology and Criminal Justice, Griffith University, 176 Messines Ridge Road, Mt Gravatt, Queensland 4122, Australia. Email: zarina@vakhitova.com
[2]Senior Lecturer, School of Criminology and Criminal Justice, Griffith University, 176 Messines Ridge Road, Mt Gravatt, Queensland 4122, Australia. Email: d.reynald@griffith.edu.au

A small body of research has tested the applicability of opportunity theories, such as the routine activity theory (Cohen & Felson, 1979) and the lifestyle exposure theory (Hindelang, Gottfriedson, & Garofalo, 1981) for modelling mechanisms of cyber abuse victimisation (Marcum, 2008; Holt & Bossler, 2009; Reyns, Henson, & Fisher, 2011; Bossler, Holt, & May, 2011). These studies found a moderate empirical support for the use of opportunity theories in the context of cyber abuse. To date cyber abuse scholarship has focused almost entirely on the victimisation perspective. Although the above mentioned studies included the guardianship factor in their models (as a predictor of victimisation), no study so far has investigated the individual and/or situational factors associated with the increased likelihood of guardianship behaviour by a bystander. The current research aims to address this gap in the literature by examining the mechanisms of guardianship against cyber abuse through the analysis of self-reports of both guardianship behaviour in response to witnessed incidents of cyber abuse.

Capable Guardianship

According to the routine activity theory (Cohen & Felson, 1979), crime is the result of the convergence of motivated offenders and suitable targets in settings where capable guardians are absent. This highlights the pivotal role of guardians as crime controllers, as it suggests that the guardian's presence or absence can ultimately alter the outcome of the crime event. It is important to emphasise here that it is the ordinary citizens performing their daily routines (and not the police, or security guards) who are considered guardians within the routine activity theory, as ordinary citizens are much more likely to be at the scene of the crime when it is occurring compared with the formal controllers (e.g., the police) (Felson, 2006).

Not all available guardians present at the scene of a crime will intervene in or even notice the crime. Felson emphasised that it is the capable guardians who can affect the outcome of a crime event (1995). So what makes a guardian capable of controlling crime? Reynald (2009, 2011) proposed the guardianship-in-action model that explains the mechanisms by which guardians can act as effective crime controllers. This model proposes four levels of guardianship intensity: the higher the intensity, the more effective the guardian is as a crime controller. Intensity 0 guardians are not visible at the crime setting and are not available for the surveillance. Intensity 1 guardians are those who are available for surveillance. Intensity 2 are guardians who are alert and aware of their surroundings. These types of guardians will probably notice a crime occurring, but may not do anything about it. Intensity 3, the final and the highest level of guardianship intensity, represents guardians who intervene when necessary. These guardians are present when a crime occurs, are aware of the crime, and are prepared to act to disrupt it directly by getting involved themselves, or indirectly by reporting it to the authorities. The guardianship-in-action classification (Reynald, 2009, 2011) makes it obvious that although availability is essential, it is not sufficient for effective guardianship. What is not entirely clear is why not all available guardians will recognise a criminal activity and why only some of those who will recognise the crime event will intervene to disrupt it.

Contextual Awareness and Willingness to Intervene

Felson (2006) argued that for guardians to be effective crime controllers they must be knowledgeable about their immediate surroundings and the context in which they could potentially perform as guardians. They must be able to recognise what they observe as a

criminal or deviant act. The basic awareness of one's situational context, *contextual awareness*, is the critical factor that determines whether available guardians are able to differentiate between normal daily routines and a criminal activity (Reynald, 2010). In the physical environment, the guardian's contextual awareness can be evident in things like the knowledge of the neighbourhood, the people who live in it, and the activities that normally occur there. Effective guardians look for cues for potential criminal activities. These cues could be people, things, and activities that are atypical of a certain context. This principle can also be applied in cyberspace, where contextual awareness could be evident in the guardian's understanding of the rules of conduct, ability to recognise prohibited behaviours, ability to differentiate between offenders and compliant users, general technological competency, and ability to locate and use help and protect oneself and others from risks associated with cyberspace.

Not only does contextual awareness play a role in available guardians' detection of potential offenders, it could also determine whether the guardian will intervene to disrupt the crime event (Felson, 2006). Reynald (2010) argued that "that the more experience and knowledge guardians have about their context, about crime and about self-protective behaviours, the more confident they will be about their capacity, and the greater their willingness to intervene" (p. 363). This suggests that contextual awareness could be the determining factor in both recognising a potential crime event and in intervening to disrupt such event. A study of guardianship by Reynald (2010) explored this idea in a residential setting and found that contextual awareness (operationalized as the guardian's ability to detect criminal activity and knowledge of the tools available for protection) is indeed associated with improved ability to recognise criminal activity. Unfortunately, it is not known how the processes of guardianship-in-action operate in the context of cyberspace or what role contextual awareness of cyberspace plays in facilitating cyber guardianship.

Guardianship against Cyber abuse

With the emergence of cyber crime, criminologists have attempted to apply terrestrial theories, such as the routine activity theory and concepts such as guardianship, to explain these new types of crime (Marcum, 2008; Holt & Bossler, 2009; Reyns, Henson, & Fisher, 2011; Bossler, Holt, & May, 2011). Cyber abuse scholarship has examined guardianship from the perspective of personal victimisation and has measured such guardianship dimensions as physical (anti-virus software and firewalls, social networking site's privacy settings and profile tracker and content-control software), social (friends pirating media, friends pirating software), personal (computer proficiency, protecting passwords), and human guardianship (restricting time online by a guardian and being monitored by a guardian while online). The measures employed by these studies reflect the non-human and/or target-hardening dimension of crime prevention rather than true guardianship as defined by Hollis et al. (2013). To date, no study has examined the situational factors that are associated with the increased likelihood of guardianship against cyber abuse.

Current Study

The current study will examine cyber stalking and cyber harassment events from the cyber guardian's perspective and will analyse self-reports of guardianship in cyberspace. For the purposes of this study, both cyber stalking and cyber harassment will be grouped

under the collective crime category of *cyber abuse* and will be defined as *the use of the Internet or other electronic means to stalk or harass an individual or a group of individuals over 18 years of age which can take the form of emails, texts, posts on web logs (blogs), forums or social networking sites of a persistent, annoying, alarming or threatening nature*. An online survey of Australian adult users of the Internet and social media forms the basis of this study. The participants were asked questions about their experiences with cyber abuse, both as witnesses and victims. Considering that the focus of the study is on cyber stalking and cyber harassment, which are defined as crimes affecting adults, the invitation to participate in this study was extended to participants aged 18 years and over[3].

In this study we extend the latest definition of guardianship in the physical world (Hollis et al., 2013) to the new environment of cyberspace and define *cyber guardianship* as *a presence of a human third party capable of deterring the would-be offender from committing a crime against an available target or acting to disrupt crime events in progress*. This definition reflects the fact that not all guardians present at the scene of a crime will intervene to disrupt the crime. We operationalize *cyber guardianship* in terms of the guardianship-in-action model (Reynald, 2010) and measure two levels of guardianship: witnessing an incident of cyber abuse (intensity 2) and intervening in the witnessed incident of cyber abuse (intensity 3). We operationalize a *cyber guardian* as any online bystander who either witnesses or acts to prevent or disrupt the incident of cyber abuse.

We hypothesise that the contextual awareness of cyberspace is a determining factor in both witnessing and intervening in incidents of cyber abuse by available cyber guardians. Knowledge of the cyber-environment not only allows potential cyber guardians to recognise cyber abuse, it also gives them the tools they need to disrupt it. *Contextual awareness of cyberspace* in this study will be measured using the following variables: (1) awareness of anti-cyber abuse policies, (2) awareness of methods of reporting cyber abuse, and (3) computer competency. Prior victimisation is used in this study as a measure related to contextual awareness, as we believe that experiencing victimisation first hand increases the victim's contextual awareness. It is not unreasonable to suggest that victimisation increases one's understanding of the crime, how it is committed, and how one can get involved in it. It is probably also likely that the victim would learn about how to protect him or herself in the future and through this process of learning would increase his or her contextual awareness in this area. Please note that as awareness of anti-cyber abuse policies and awareness of methods of reporting cyber abuse are related to the witnessed incidents of cyber abuse, these two variables were excluded from analyses that examine cyber guardianship intensity 2 (witnessing cyber abuse).

To build on existing knowledge on the guardianship-in-action processes in the context of cyberspace, this research attempts to answer the following research questions:

1. Who are the cyber guardians? What individual characteristics of guardians, if any, are associated with witnessing and intervening in incidents of cyber abuse?
2. What role, if any, does contextual awareness of cyberspace play in witnessing incidents of cyber abuse by available cyber guardians?
3. What role, if any, does contextual awareness of cyberspace play in intervention in incidents of cyber abuse by cyber guardians?

[3] Acts of online harassment and online stalking in which victims are under 18 years of age are generally referred to as cyber bullying.

Data and Methodology

To answer the research questions, we conducted an online survey of guardianship against cyber abuse using the Survey Monkey platform (http://www.surveymonkey.com). The survey was designed to acquire information related to participants' experiences with cyber abuse incidents. The questions asked about two types of incidents of cyber abuse: those that were experienced by participants (1) as bystanders (witnesses or interveners) and (2) as victims. Using the online survey, a sample of Australian adults (18 years of age and older) was drawn from a large non-probability panel. As respondents who participate in such panels tend to differ from the general population (Internet users are more likely to be younger, to be better educated, and to have higher income (Baker et al., 2010)), non-probability online samples are not generally considered appropriate for making inferences about the prevalence of phenomena occurring in the general population (Pickett et al., 2013). However, non-probability samples can and have been successfully used for evaluating theories (Picket et al., 2013; Broidy, 2001; Hay, 2001; Stets & Carter, 2012; Van Gelder & de Vries, 2012): "data from non-probability samples can provide important insights into a theory's empirical plausibility, after which subsequent studies can begin to identify whether its explanatory power varies across social groups" (Picket et al., 2013, p. 737). Moreover, cyber abuse, the focus of the current study, is one of more suitable criminological phenomena for being explored using an online panel, as having access to the Internet is the necessary requirement for becoming involved in cyber abuse in any capacity.

Besides being a valuable method of testing theories, the use of online samples has other advantages. Compared with surveys conducted using telephone or face-to-face interviews, online surveys are associated with reduced interviewer-induced measurement error: the respondents can answer questions in the comfort of their homes, are able to read the questions, and do not have to memorise the possible answers for multiple-choice questions (Baker et al., 2010; Sue & Ritter, 2012). Online surveys also appear to produce less social desirability bias compared with interviewer-assisted surveys (Chang & Krosnick, 2009; Kreuter et al., 2008). Several studies have compared the findings from non-probability online samples and from probability phone and face-to-face interview samples: both were found to produce very similar relational inferences (Berrens et al., 2003; Sanders et al., 2007; Stephenson & Crete, 2010). In summary, as long as online surveys of non-probability panels are used appropriately (e.g., for testing theories), they offer a cost-effective and fast way of collecting data (Bethlehem & Biffignandi, 2012), comparable with probability samples (Berrens et al., 2003; Sanders et al., 2007; Stephenson & Crete, 2010).

Population and Sample

The target population in this study consisted of Australian adult users of the Internet and social media sites. Over 80% of Australian households are connected to the Internet (ABS, 2013). Australian Internet and social media users tend to be younger (over 95% of Australians in the 15-34 years age group category and only 46% of those over 65 years are Internet users), are better educated (96% of Bachelor or above degree holders were Internet users), and are as likely to be male as female (84% compared with 83%, respectively) (ABS, 2013). Majority of Australian Internet users (81%) reported possessing at least average (45%) to above average (36%) computer competency ("Australian Communications and Media Authority", 2009). Sixty-five percent of online Australians use one or more social media sites (Glass, 2014), and a majority of social media users (97%)

have an account with Facebook, which is by far the most popular social media site in Australia.

In total, 650 respondents participated in this study. Participants were selected from Survey Monkey Audience[4] (an online panel) using a purposive quota sampling method based on the following selection criteria: (1) Australian residents, (2) 18 years of age or over, and (3) users of the Internet. Participants were e-mailed a generic Survey Monkey invitation that did not include any specific information about the survey topic to reduce the possibility of the response bias that could potentially lead to overrepresentation of the respondents especially concerned with cyber abuse.[5] Out of 650 respondents who clicked on the link provided in the e-mail invitation and started the survey, 604 (93%) respondents completed the survey[6]. The respondents who did not complete the survey were included in the total sample and were treated as records with missing data.

Table 1 presents descriptive analyses of the key variables measured in the survey. The final sample used in the analyses consisted of participants between the ages of 18 and 67 (M = 37, SD = 11.38), 60% of the sample being 35 years of age or older. Because the survey was administered to an online panel using a quota sampling method, it was difficult to control who responded; as a result, males are underrepresented (25%) in the sample. Of the respondents, 42% indicated that they completed undergraduate or postgraduate studies. The respondents were quite evenly distributed across occupational categories, with the two most common categories being university/college students (17%) and in the service/customer support/sales/marketing category (13%). The majority of users (86%) reported intermediate (48%) or advanced (38%) levels of computer competency. Facebook was a social media site of choice for 70% of respondents. In summary, respondents in our sample were more likely to be slightly older, female, better educated, competent computer users, students or service industry employees, and Facebook users. As often happens with non-probability samples, the final sample differs in some aspects (gender and age) from the target population, while it is very similar in others (education and computer competency). Considering that one of the goals of the study was to test the predictive power of contextual awareness in cyberspace, having a sample similar to the target population in terms of computer competency (one of the variables used to measure contextual awareness) improves the validity of potential findings.

[4] Survey Monkey Audience recruits panellists through the company's online advertising. As an incentive to participate in surveys, Survey Monkey offers its panellists charity donations on their behalf and/or a chance to win $100 in weekly drawings. Survey Monkey employs several measures to ensure quality of responses: panellists are limited to two surveys per week; an IP-tracking software is used to prevent the possibility of duplicate respondents; individuals implicated in inappropriate responding behaviour are removed from the panel.

[5] In addition, Tourangeau and colleagues (2009) found that in online surveys, the topic of the survey does not influence the panellists' decision to participate.

[6] Due to the way Survey Monkey invites their panellists to participate in their surveys (a number of e-mail invitations, usually 10 times the quota, are sent out simultaneously; the collector closes as soon as quota is reached), we cannot estimate the response rate for this survey. Survey Monkey estimates average response rate to be between 10% and 20%. Although certainly on the low side, the potentially low response rate was not a concern in this study. Keeter et al. (2000) compared the results of two identical surveys administered with two randomly selected groups. In one survey the researchers made an effort to increase the response rate (which resulted in a 65% response rate) and did not make such effort in the other (which received response from 36% of potential respondents). Despite significantly different response rates, the demographic makeup of the respondents and their responses in both groups were remarkably similar.

Table 1. Descriptive Statistics for Variables of Interest

Variable	*M*	*SD*	*n*	*%*
DEPENDENT VARIABLES				
Intervention in cyber abuse	.51	.50	208	
0 - No			101	39.30
1 - Yes			107	41.63
Witnessing cyber abuse	.40	.49	650	100.00
0 - No			393	60.46
1 - Yes			257	39.54
INDEPENDENT VARIABLES				
Demographics				
Age (18-67)	37.52	11.38	583	
1 – 18-24 years of age			42	7.2
2 – 25-34 years of age			121	20.8
3 – 35-44 years of age			142	24.4
4 – 45-54 years of age			176	30.2
5 – 55-67 years of age			102	17.5
Gender	.26	0.44		
0 - Female			464	74.50
1 – Male			159	25.50
Occupation[7]			619	
College/graduate student			102	16.50
Homemaker			83	13.40
Service/customer support/sales			80	12.90
Education	5.08	1.28	623	
Primary school			1	.20
Some secondary school			62	10.00
Completed secondary school			193	31.00
Trade training			103	16.50
Undergraduate university			161	25.80
Postgraduate university			103	16.50
Contextual Awareness				
Awareness of anti-cyber abuse policies[8]	.50	.50	255	
0 - Not aware of policy			127	49.80
1 - Aware of policy			128	50.20
Awareness of method of reporting of cyber abuse[9]	.75	.43	255	
0 - Not aware of method			64	25.10
1 - Aware of method			191	74.90
Level of computer competency	3.48	.74	621	
1 - I am new to computers			2	0.30
2 - Beginner level			36	5.80
3 - Intermediate level			298	48.00
4 - Advanced level			233	37.50
5 - Expert level			52	8.40
Prior victimization	.20	.40	590	
0 - No			474	80.30
1 – Yes			116	19.70

[7] Most common categories.
[8] In relation to witnessed incident of cyber abuse.
[9] In relation to witnessed incident of cyber abuse.

Dependent Variables

To examine how guardianship operates in cyberspace, we created two dependent binary variables: witnessing an event of cyber abuse and intervening in an event of cyber abuse (see Table 2). These two variables represent different levels of guardianship intensity according to the guardianship-in-action model - intensity 2 (witnessing) and 3 (intervention) (Reynald, 2010). The witnessing variable is operationalized as personally witnessing an incident when someone other than the respondent is harassed or stalked online (not read about it in the newspaper, or seen in the news). The original question included three possible options: 1 – "yes, once"; 2 – "yes, more than once"; 3 – "No, never". We decided to code this into a binary variable with options 1 and 2, coded as 1 – "yes", and option 3 coded as 0 – "no". The intervention variable is operationalized as any active involvement by a third party in the incident of cyber abuse by either reporting to the police, the social media site, or the Internet service provider, by contacting the offender and/or the victim, or by any other involvement with the goal of disrupting the cyber abuse event. The three possible answers included 1 – "yes", 2 – "no", 3 – "prefer not to disclose". From the original answers we created a binary variable with two categories: 1 – "yes" and 0 – "no". Option 3 was coded as missing values.

Independent Variables

The focus of this study is on individual and/or situational factors that predict guardianship in the form of witnessing and intervening in incidents of cyber abuse. To answer the research questions we created several independent variables, including demographic, contextual awareness, and prior victimisation variables (see Table 3). *Demographic factors* included gender (0 – male, 1 – female), age, education, and occupation. *Age* was measured as a categorical variable: 1 – "18 to 24 years of age"; 2 – "25 to 34 years of age"; 3 – "35 to 44 years of age"; 4 – "45 to 54 years of age"; 5 – "55 to 67 years of age". The *education* variable had the following categories: 1 – "did not attend school"; 2 – "primary school"; 3 – "some secondary school"; 4 – "completed secondary school"; 5 – "trade training"; 6 – "undergraduate university"; 7 – "postgraduate university". The *occupation* variable included the following categories: 1 – "executive/managerial"; 2 – "professional (doctor, lawyer, etc.)"; 3 – "academic/educator"; 4 – "technical/engineering"; 5 – "police officer"; 6 – "army, navy, marine"; 7 – "service/customer support/sales/marketing"; 8 – "clerical/administrative"; 9 – "tradesman/craftsman"; 10 – "college/graduate student"; 11 – "homemaker"; 12 – "self-employed/own company"; 13 – "unemployed/looking for work"; 14 – "retired". The *education* and *occupation* variables were recoded into several binary variables where each profession or level of education was turned into a separate variable, for example, "college/graduate student": 0 – no, 1 – yes.

Contextual awareness in cyberspace was operationalized as (1) awareness of anti-cyber abuse policies, (2) awareness of methods of reporting cyber abuse, and (3) computer competency. Awareness of anti-cyber abuse policies was constructed from the question, "Does the provider where you witnessed an incident of cyber abuse have a policy on cyber abuse or code of conduct covering cyber stalking and/or cyber harassment?" If the respondent answered 1 – "yes" or 2 – "no", this was recoded into 1 – "aware of policy". If the respondent answered 3 – "I don't know", this was recoded into 0 – "not aware of policy". Awareness of methods of reporting cyber abuse was constructed similarly to awareness of anti-cyber abuse policies from question, "Does the provider where you

witnessed an incident of cyber abuse have a method of reporting cyber abuse?" Computer competency was constructed from the item, "Please rate your level of competency in using the Internet and computer technologies," as a five-point scale variable with the following values: 1 – "I am new to computers"; 2 – "beginner level"; 3 – "intermediate level"; 4 – "advanced level"; and 5 – "expert level".

Prior victimisation was operationalized as directly experiencing cyber stalking or cyber harassment. The prior victimisation variable was constructed as a binary variable from the question, "Have you ever experienced cyber abuse directly?" The respondents were provided with the definition and examples of cyber abuse: "unwanted, annoying, harassing or threatening e-mails, text messages, instant messages (IM); embarrassing, defamatory, tormenting posts on online forums, blogs, entries on web sites, online games; hacking into your e-mail or social networking site (such as Facebook) account and changing entries to embarrass you; impersonating you and posting false information on online forums; unauthorised registration for unwanted services (e.g. spam, adult material sites); breaking into your e-mail account and sending out obscene or hurtful messages to people in your address book."

Results

The main goal of this study was to test the hypothesis that contextual awareness of cyberspace increases the likelihood of both witnessing and intervening in incidents of cyber abuse. As both dependent variables in this study are binary variables, we employed binary logistic regression to test the hypothesis. Pair wise exclusion of cases was used in all analyses involving variables with missing data. The variables included in regression models were tested for potential problems with multicollinearity/singularity, and none such problems were detected. To uncover any potentially valuable interactions between main effects that are not revealed through regression analysis, we produced two-way plots of interaction between the main effect variables.

Individual Characteristics of Cyber guardians

Out of 650 respondents, nearly 40% (n = 257) reported witnessing an incident of cyber abuse one or more times, and 16% (n = 107) (41% of those who witnessed cyber abuse), reported intervention in those incidents of cyber abuse. The majority of interveners took action by reporting the incident(s) to the social media site's administrators (42%, n = 45). Whereas 40% of the total sample reported witnessing at least one incident of cyber abuse, only 19% of the total sample reported experiencing cyber abuse first hand as victims.

Table 2 presents the descriptive statistics for different groups of bystanders: witnesses, non-witnesses, interveners and non-interveners. A Mann-Whitney U Test revealed that witnesses were significantly different from non-witnesses in terms of their age: U = 27185.00, z = -6.83, p = .000, r = 0.28 (medium effect according to Cohen (1988)). There was also a statistically significant age difference between interveners and non-interveners: U = 3983.00, z = -2.05, p = 0.04, although the effect was smaller: r = 0.15. A Chi-square test for independence with Yates' correction for continuity revealed no significant association between gender and witnessing (χ^2 (1, n = 623) = .08, p = .77, *phi* = -.02) or intervention (χ^2 (1, n = 204) = .09, p = .77, *phi* = -.03). In other words, gender was not a determining factor in witnessing or intervening in incidents of cyber abuse.

While witnesses were significantly more computer competent compared to non-witnesses: U = 35830.50, z = -5.12, p = .000, r = .21, there was no significant difference

in computer competency scores between interveners and non-interveners: $U = 4912.50$, $z = -.48$, $p = .631$, $r = .03$. In terms of education, most witnesses and interveners reported having "completed secondary school" (30% and 33% respectively) and "undergraduate university/college" (29% and 26% respectively). University students made up 23% of witnesses and 24% of interveners, whereas "service/ customer support/ sales/ marketing" was the second most common occupation (13% of witnesses and 15% of interveners).

Table 2. *Descriptive Statistics for Interveners and Non-Interveners*

Variable	*Witnesses (n =257)*	*Non-Witnesses (n = 392)*	*Interveners* (n = 106)*	*Non-Interveners* (n = 100)*
Age	(*n* = 233)	(*n* = 350)	(*n* = 102)	(*n* = 94)
Mean	34.55 ± 11.54	40.17 ± 10.48	35.07 ± 11.70	31.86 ± 11.43
Median	32	42	35	29
Range	18 - 67	18 - 65	18 – 58	18 – 67
Gender	(*n* = 247)	(*n* = 376)	(*n* = 106)	(*n* = 98)
Male	24.70%	26.10%	20.80%	23.50%
Female	75.30%	73.90%	79.20%	76.50%
Education Level**	(*n* = 247)	(*n* = 376)	(*n* = 106)	(*n* = 98)
Completed secondary school	30.40%	31.40%	33.00%	28.60%
Undergraduate university	29.10%	23.70%	25.50%	31.60%

Variable	*Witnesses*	*Non-Witnesses*	*Interveners**	*Non-Interveners**
Occupation**	(*n* = 246)	(*n* = 373)	(*n* = 106)	(*n* = 98)
College/graduate student	23.20%	12.10%	23.60%	25.50%
Service/ customer support/ sales	13.00%	12.90%	15.10%	11.20%
Clerical/ administrative	10.60%	13.70%	5.70%	17.30%
Homemaker	12.20%	14.20%	12.10%	9.20%
Computer Competency Level	(n = 245)	(n = 376)	(n = 104)	(n = 98)
Mean	3.67 ± .72	3.35 ± .73	3.67 ± .74	3.72 ± .70
Median	4	3	4	4

* *Subset of Witnesses*
** *Most common category*

Contextual Awareness and Witnessing of the Incidents of Cyber abuse

As illustrated in Table 3, prior victimisation, computer competency, and age all emerged as significant predictors of witnessing incidents of cyber abuse. The strongest variable explaining the variance in witnessing cyber abuse was prior victimisation ($OR = 8.8$, $p = .000$). These results indicate that the odds of witnessing cyber abuse are nearly 9 times greater for respondents who were prior victims of cyber abuse than those who were not. Furthermore, the odds were 1.5 times greater for more competent computer users than for less competent users. Analyses showed that prior victimisation, computer competency, and age together explain 30% of the variance in witnessing cyber abuse.

To explore any potentially valuable interactions between the main effect variables, we produced two-way interaction plots between age, prior victimisation, and computer competency variables. As Figure 1 shows, there appears to be no interaction between age and prior victimisation, and between age and computer competency. Age does appear to interact slightly with computer competency, but this interaction is not statistically significant ($OR = .65$, $p = .29$).

Table 3. Model 1: Binary Logistic Regression Predicting the Likelihood of Witnessing in Cyber abuse

Variable	*B*	*S.E.*	*Exp(B)*
Prior cyber abuse victimisation	2.18***	.27	8.81
Computer competency	.44**	.14	1.55
Age	-.34**	.09	.71

** p < .05. ** p < .01. *** p < .001 (two-tailed significance test)*
*- 2 log ll = 595.86; Model Chi-square = 134.55***; Nagelkerke R squared = .30; n = 547*

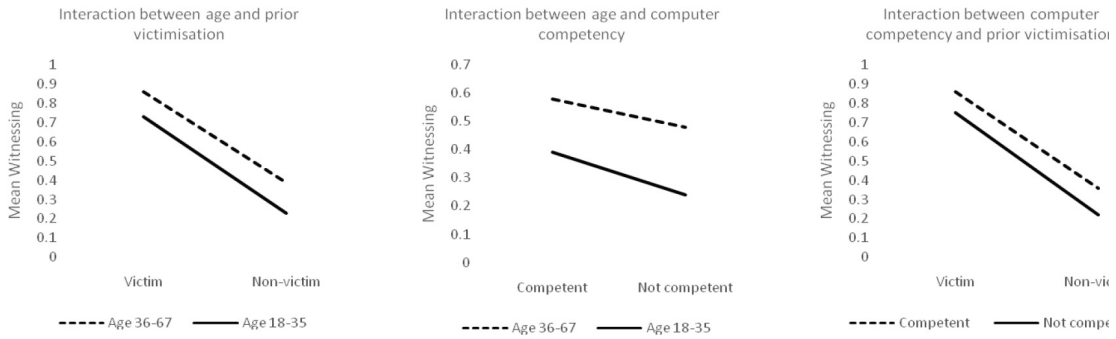

Figure 1. Interaction plots for witnessing cyberabuse

Table 4. Model 2: Binary Logistic Regression Predicting the Likelihood of Intervention in Cyber abuse

Variable	*B*	*S.E.*	*Exp(B)*
Awareness of anti-cyber abuse policies	.69*	.34	1.99
Awareness of methods of reporting	.39	.42	1.47
Prior cyber abuse victimisation	.93**	.33	2.52
Computer competency	-.18	.22	.83
Age	.37**	.14	1.44

** p < .05. ** p < .01. *** p < .001 (two-tailed significance test)*
*- 2 log ll = 229.07; Model Chi-square = 21.71**; Nagelkerke R squared = .15; n = 181*

Contextual Awareness and Intervention in the Incidents of Cyber abuse

Next, we turn our attention to factors that explain intervention. As we can see from Table 4, prior victimisation, age, and awareness of anti-cyber abuse policies are the only variables that make a statistically significant contribution. Prior victimisation is the strongest explanatory variable for reporting intervening in incidents of cyber abuse: respondents who reported prior victimization had 2.5 times greater odds of intervening in cyber abuse than those who did not. Respondents who were aware of anti-cyber abuse policy had 2 times greater odds of intervention in cyber abuse incident than those who were not aware.

Two-way interaction plots (Figure 2) suggest that all three main effect variables interact with each other to some degree. Interaction between age and prior victimisation is the strongest of the three and is the only one that emerges as statistically significant (OR = 5.34, p = .01). In this interaction younger and older victims have almost identical intervention means (M = .64 vs. M = .63), but the same is not true for non-victims: older non-victims appear to be much more likely to intervene (M = .62) than younger non-victims (M = .27).

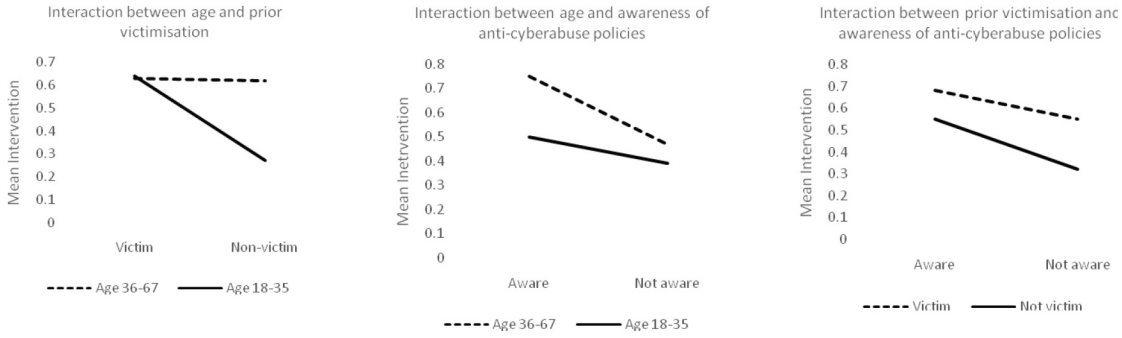

Figure 2. Interaction plots for intervention in cyberabuse

In summary, we found that the respondents who intervened in incidents of cyber abuse were demographically very similar to those who did not intervene, and those who witnessed cyber abuse did not differ much from those who did not. We were able to confirm the hypothesis that contextual awareness of cyberspace increases the probability of both witnessing and intervening in incidents of cyber abuse: we found that the more competent computer users were more likely to witness cyber abuse, whereas users who were aware of anti-cyber abuse policies were more likely to intervene, after controlling for the age of respondents. Prior victimisation, which was used as a measure related to contextual awareness, was found to be predictive of witnessing, but had a more complex, interactive (via age) relationship with intervention.

Discussion and Conclusion

One of the underlying goals of this study was to gather empirical evidence to establish the function and characteristics of cyber guardians. This study revealed that cyber guardians, like guardians (Reynald, 2010), are an anomalous group of ordinary people. There is no occupation or level of education that is unique to guardians who take action

to intervene when they witness cyber abuse. Cyber guardians are equally as likely to be male as female. Age plays an interesting role in cyber guardianship: younger guardians are more likely than older ones to witness incidents of cyber abuse, but as the intensity of guardianship increases, the effect of age changes and it is the older guardians who are more likely to intervene.

Considering that cyberspace is quite different from the physical world, it was expected that factors that facilitate guardianship in cyberspace may also be different. The results show, however, that active guardianship processes in cyberspace operate in a remarkably similar fashion to the physical world. In the physical world, contextual awareness of the surrounding environment was found to be a critical factor affecting the guardian's decision-making process (Felson, 2006; Reynald, 2010). In this study, contextual awareness was found to be predictive of both witnessing cyber abuse and intervening in incidents of cyber abuse. We argued that factors such as computer competency, awareness of policy, and prior victimisation all contribute to contextual awareness, or the understanding and the knowledge of the environment, and, therefore, provide strong indicators of this concept. Computer competency is a good indicator of guardians' ability to navigate the environment (cyberspace). Awareness of anti-cyber stalking policies is reflective of the guardian's knowledge of rules and laws of cyberspace, as the purpose of anti-cyber stalking policies is to set out what is allowed and what is prohibited in cyberspace. Prior victimisation can also be viewed as adding to guardians' ability to recognise certain actions as unlawful through direct previous experience. We found that computer competency increases the likelihood of witnessing, but as the intensity of guardianship increases, it becomes less important: computer competency is not predictive of intervention. On the other hand, awareness of anti-cyber abuse policies is what distinguishes guardians who witness cyber abuse, but do nothing to disrupt it, from those who actively intervene. We believe that awareness of anti-cyber abuse policies is reflective of a more specialised knowledge compared with general computer and Internet knowledge. This finding suggests that contextual awareness follows the path of guardianship: as guardianship intensity increases, so does the intensity or depth of associated knowledge. To witness an incident of cyber abuse, it is enough to be a competent computer user, but intervention is associated with a much more specialised knowledge. In summary, this study established that contextual awareness of cyberspace is predictive of both witnessing and intervening in incidents or cyber abuse, and as the cyber guardianship intensity increases, so does the intensity of contextual awareness.

One interesting finding from this study is that prior victimisation and age have a complex interactive relationship with intervention. Older respondents were not affected by prior victimisation, whereas younger victims reported much lower rates of intervention than younger non-victims. It is not clear why prior victimisation would have such effect on younger but not older cyber guardians. This finding is surprising and requires further investigation.

The results from this study show a clear association between cyber abuse victimisation and guardianship. One issue in interpreting these findings is our lack of knowledge about the time order of the events of witnessing and intervening in an incident cyber abuse, and becoming a victim. We therefore cannot make conclusions about the directionality of detected associations. From our data we do not know whether it is victimisation that facilitates guardianship or that guardians are more likely to be victimised. If victimisation precedes guardianship, then we could hypothesise that people who experience

victimisation first-hand may be more likely not only to recognise events as a criminal activity but also to empathise with another individual in a similar situation. Prior victims are also likely to be more knowledgeable about how to deal with such situations due to their previous exposure to victimisation. If, on the other hand, guardianship preceded victimisation, the explanation may lie in the guardians' exposure to risky environments. While attempting to disrupt an incident of cyber abuse, guardians increase their own risk of cyber-attacks, especially if they contact the abuser directly. Further research is required to disentangle these processes.

Theoretical and Policy Implications

This study contributes to the existing literature by bringing the research on guardianship in the physical world to the unique setting of cyberspace by examining the role of contextual awareness in the cyber guardian's decision-making process. In its original formulation, the routine activity theory postulates that crime can be prevented just by someone being there at the scene of the crime when the crime is occurring (Cohen & Felson, 1979). As has been demonstrated in the physical world, this study presents evidence to support the idea that the availability of guardians is not sufficient to discourage or disrupt crime or related events (Felson, 2006). Existing research suggests that a critical factor that distinguishes available guardians from actively intervening ones is contextual awareness of the surrounding environment (Felson, 2006; Reynald, 2011). This study shows that, despite obvious differences in environment, guardianship in cyberspace appears to work in a similar way to how it operates in the physical world and that contextual awareness is a critical factor in both witnessing and intervening in incidents of cyber abuse.

The existing literature proposes having anti-cyber abuse policies and methods of reporting as one of the main methods of situational crime prevention in cyberspace (Reyns, 2010). Our findings suggest that a more fundamental function of cyberspace managers (managers and developers of social media sites and Internet service providers, etc.) is to help facilitate capable guardianship by increasing guardians' contextual awareness of cyberspace. There are many ways in which this education of online users about their important role in crime control in cyberspace could be accomplished. For example, social media sites could display public ads describing cyber abuse, its consequences to the victims, and what ordinary bystanders could do to stop it.

In closing, we reiterate that the sample used in this study was obtained from a non-probability panel, which limits the generalizability of findings. As the purpose of this study was to test a theoretical supposition, the use of non-probability sample was justified, but further research is needed to examine whether the patterns revealed in this study are representative of the general population of Australian Internet users.

Acknowledgement

The authors would like to thank Professor Henk Elffers (NSCR) for his critical feedback on an earlier draft of the paper.

References

Australian Bureau of Statistics (ABS). (2013). 8146.0 - Household use of information technology, Australia, 2012-13.

Australian Communications and Media Authority (ACMA). (2009). Australia in the digital economy. Report 1: Trust and confidence. Retrieved on July 12, 2014 from

http://www.acma.gov.au/webwr/aba/about/recruitment/trust_and_confidence_aust_in_digital_economy.pdf

Baker, R., Blumberg, S. J., Brick, J.M., Couper, M. P. Courtright, M., Dennis, J. M., Dillman, D., Frankel, M. R., Garland, P. Groves, R. M., Kennedy, C., Kroskick, J., Lavrakas, P. J. (2010). Research synthesis: AAPOR report on online panels. *Public Opinion Quarterly, 74*, 711–781.

Beran, T., & Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. *Journal of Educational Computing Research*, *32*, 265–277.

Berrens, R. P., Bohara, A. K., Jenkins-Smith, H., Silva, C., & Weimer, D. L. (2003). The advent of Internet surveys for political research: A comparison of telephone and Internet samples. *Political Analysis, 11,* 1–22.

Bethlehem, J., & Biffignandi, S. (2012). *Handbook of Web surveys. Wiley handbooks in survey methodology.* New Jersey: John Wiley & Sons. ISBN 978-1-118-12172-6.

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

Bossler, A. M., Holt, T. J., & May, D. C. (2011). Predicting online harassment victimisation among juvenile population. *Youth Society, 44*, 500–523.

Broidy, L. M. (2001). A test of general strain theory. *Criminology, 39*, 9–35.

Chang, L., & Krosnick, J. A. (2009). National surveys via RDD telephone interviewing versus the Internet: Comparing sample representativeness and response quality. *Public Opinion Quarterly, 73*, 641–678.

Cohen, J. W. (1988). *Statistical power analysis for the behavioural sciences* (2nd edn). Hillsdale, NJ: Lawrence Erlbaum Associates.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588–608.

Erdur-Baker, O. (2010). Cyberbullying and its correlation to traditional bullying, gender and frequent risky usage of Internet-mediated communication tools. *New Media Society, 12*, 109–125.

Felson, M. (1995). Those who discourage crime. In J. E. Eck & D. Weisburd (eds.), *Crime and Place (pp.* 53–66). Monsey, NY: Criminal Justice Press.

Felson, M. (2006). *Crime and Nature.* Thousand Oaks, CA: Sage.

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence, 19*(4), 468–483.

Glass, D. (2013). Aussies are getting socially mobile while businesses miss the mark! Sensis. Retrieved on February 15, 2014 from http://about.sensis.com.au/News/Media-Releases/?ItemID=1225&count=1.

Hay, C. (2001). Parenting, self-control, and delinquency: A test of self-control theory. *Criminology, 39*, 707–736.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (2010). *Victims of Personal crime: An Empirical Foundation for a Theory of Personal Victimisation.* Cambridge, MA: Ballinger.

Hinduja, S., & Patchin, J. W. (2009). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying.* New York: Corwin Press.

Hokoda, A., Hsuch-Huei Lu, H., & Angeles, M. (2006). School bullying in Taiwanese adolescents. *Journal of Emotional Abuse, 6*, 69–90.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cyber crime victimisation. *Deviant Behaviour, 30*, 1–25.

Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety*, *15*(1), 65–79.

Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2012). Trends in youth Internet victimization: Findings from three youth Internet safety surveys 2000–2010. *Journal of Adolescent Health, 50*, 179–186.

Keeter, S., Miller, C., Kohut, A., Groves, R., & Presser, S. (2000). Consequences of reducing nonresponse in a large national telephone survey. *Public Opinion Quarterly*, *64*, 125–148.

Kreuter, F., Presser, S., & Tourangeau, R. (2008). Social desirability bias in CATI, IVR and Web surveys: The effect of mode and question sensitivity. *Public Opinion Quarterly, 72*, 847–865.

Marcum, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology*, *2*(2), 346–67.

Picket, T. J., Mancini, C., & Mears, D. P. (2013). Vulnerable victims, monstrous offenders, and unmanageable risk: Explaining public opinion on the social control of sex crime. *Criminology, 51*(3), 729–759.

Reynald, D. M. (2009). Guardianship in action: Developing a new tool for measurement. *Crime Prevention and Community Safety*, *11*(1), 1–20.

Reynald, D. M. (2010). Guardians on guardianship: Factors affecting the willingness to monitor, the ability to detect potential offenders and the willingness to intervene. *Journal of Research in Crime and Delinquency*, *47*(3), 358–390.

Reynald, D. M. (2011). *Guarding against crime: Measuring guardianship within routine activity theory*. Farnham, UK: Ashgate.

Reyns, B. W. (2010). A situational crime prevention approach to cyber stalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety*, *12*(2), 99–118.

Reyns, B. W., Henson, B., & Fisher, B. (2011). Being pursued online: applying cyberlifestyle-routine activities theory to cyber stalking victimisation. *Criminal Justice and Behaviour, 38,* 1149–1169.

Reyns, B. W., Henson, B., & Fisher, B.S. (2012). Stalking in the twilight zone: Extent of cyber stalking victimization and offending among college students. *Deviant Behavior, 33,* 1–25.

Sanders, D. Clarke, H. D., Stewart, M. C., & Whiteley, P. (2007). Does mode matter for modelling political choice? Evidence from the 2005 British Election Study. *Political Analysis, 15,* 257–285.

Stephenson, L. B., & Crete, J. (2010). Studying political behaviour: A comparison of internet and telephone surveys. *International Journal of Public Opinion Research, 23*, 24–55.