Cyberstalking: Investigating formal intervention and the role of corporate social responsibility

Cyberstalking: Investigating Formal Intervention and the Role of Corporate Social Responsibility

*Haider M. al-Khateeb * [1, 2], Gregory Epiphaniou [2], Zhraa A. Alhaboby [1,3], James Barnes [1,], Emma Short [1]*

haider.alkhateeb@beds.ac.uk, gregory.epiphaniou@beds.ac.uk, zhraa.alhaboby@beds.ac.uk, james.barnes@beds.ac.uk, emma.short@beds.ac.uk

[1] National Centre for Cyberstalking Research, University of Bedfordshire, UK
[2] Institute for Research in Applicable Computing, University of Bedfordshire, UK
[3] Institute for Health Research, University of Bedfordshire, UK

*Corresponding Author

Abstract—

Context: Online harassment and stalking have been identified with growing accordance as anti-social behaviours, potentially with extreme consequences including indirect or direct physical injury, emotional distress and/or financial loss.

Objective: As part of our ongoing work to research and establish better understanding of cyberstalking, this study aims to investigate the role of Police, Mobile Operators, Internet Service Providers (ISPs) and owners/administrators of online platforms (e.g. websites, chatrooms) in terms of intervention in response to offences. We ask to what different authorities do people report incidents of cyberstalking? Do these authorities provide satisfactory responses or interventions? And how can this be improved? Furthermore, we discuss the role of Corporate Social Responsibility (CSR) to encourage the implementation of cyberstalking-aware schemes by service providers to support victims. In addition, CSR can be used as a means to measure the effects of externality factor in dictating the relationship between the impact of a given individuals' privacy loss and strategic decisions on investment to security controls in an organisational context.

Method: A Mixed design method has been used in this study. Data collection took place by means of an online survey made available for three years to record both qualitative and quantitative data. Overall, 305 participants responded from which 274 identified themselves as victims of online harassment.

Result: Our results suggest that most offences were communicated through private channels such as emails and/or mobile texts/calls. A significant number of victims did not report this to their service provider because they did not know they could. While Police were recognised as the first-point-of-contact in such cases, 41.6% of our sample did not contact the Police due to reasons such as fear of escalation, guilt/sympathy and self-blaming. Experiences from those who have reported offences to service providers demonstrate that no or very little support was offered. Overall, the majority of participants shared the view that third-party intervention is required on their behalf in order to mitigate risks associated with cyberstalking. An independent specialist anti-stalking organisation was a popular choice to act on their behalf followed by the Police and network providers.

Conclusion: Incidents are taking place on channels owned and controlled by large, cross-border international companies providing mobile services, webmail and social networking. The lack of support offered to victims in many cases of cyberstalking can be identified as Corporate Social Irresponsibility (CSI). We anticipate that awareness should be raised as regarding service providers' liability and social responsibility towards adopting better strategies.

Keywords: Cyberstalking, Online harassment, Incident Response, Police, Service Provider, Corporate Social Responsibility

1. Introduction

Although there is no conclusive evidence as to the increasing prevalence of cyberstalking on account of advancements in technology, it can be assumed that the number of cyberstalking incidents has indeed risen dramatically. Cyberstalking prevalence ranges from 3.2% to 82% depending on the context and criteria adopted

doi:10.1016/j.tele.2016.08.016

to identify cases (Dreßing, Bailer et al. 2014). According to a report released by the United Nation's International Telecommunication Union (ITU) (2013), approximately 39% of the world's population now has access to the Internet, which is equivalent to around 2.7 billion people. There is significant evidence to suggest new "Netizens" joining the Internet every day with limited knowledge about security threats and the implications of their online activities for their privacy and security. This estimate is subjected to regional variations, the Office for National Statistics reported that 86% of households in Great Britain had internet access in 2015, representing 22.5 million users (ONS 2015). However, while this trend is certainly beneficial in many ways, increased Internet availability can also have some negative implications, particularly as the increasing quantity of online data and correspondence has enabled large-scale illegal and unethical activity with an exponential increase of the attack surface utilised by perpetrators. Online resources can also be utilised unlawfully by criminals. For instance, with regard to cyberstalking, criminals can access a large number of online users to stalk or harass using several attack vectors including social media. The Protection from Harassment Act (PHA) in the UK (CPS 1997) defines harassment (Section 2), stalking (Section 2a) and fear of violence (Section 4) as any act that occurs more than once which leads to the severe distress or anxiety of the victim and/or hinders their ability to go about their daily lives (Section 4a); this act requires the offender to have full knowledge that their actions or behaviour is indicative of harassment, stalking and/or fear of violence (Home Office 2012).

The majority of psychiatric studies regard stalking in a similar light by referring to it as any action or behaviour in which an offender continually intrudes on the life of another to the extent that the recipient feels distressed or unsafe as a result (Mullen, Pathé et al. 2004, Strawhun, Adams et al. 2013). Furthermore, stalking is characterised by repeated unwelcomed advances and persistent intrusive behaviour. In terms of how continued intrusion can be regarded as a criminal issue, the distinction between normal and abnormal contact is defined as any continual intrusions that take place over the course of a month on at least 10 separate occasions (Pathe, Mullen et al. 2000). While there are no cohesive guidelines regarding what can be constituted as an online-based intrusion, proximal definitions are generally also applied to cyberstalking.

Individuals may experience physical or long term mental illness (Kropp, Hart et al. 2011) if they are victims of cyberstalking. Stalking was found to be associated with negative health consequences for both male and female victims including anxiety, flashbacks, headache, gastrointestinal symptoms, eating disorder and weight fluctuations and excessive tiredness, in addition to smoking and excessive drinking (Path and Mullen 1997, Sheridan, Davies et al. 2001, Dreßing, Bailer et al. 2014). Direct physical effects resulting from violence were documented but it was found that fear of violence and the unpredictable nature of intrusions have more impact on health such as Post Traumatic Stress Disorder (PTSD) (Davis, Coker et al. 2002, Pittaro 2007, Maass, Cadinu et al. 2013). PTSD is a condition that develops after experiencing an extremely stressful event. It is characterised by repetitive recalling of the stressful experience such as flashbacks of the stressor or nightmares, avoiding people or situations related to the stressor, changes in mood and cognition and symptoms of increased psychological activity (WHO 1992).

In many cases, physical harm is a serious concern or consequence. However, cyberstalking can generate even greater anxiety as the offender makes the transition from online stalking to making physical contact with the victim. In fact, it is often likely that the victim was introduced to the perpetrator in real life before the latter began to stalk them online (Maple, Short et al. 2012). Nonetheless, there are also instances where the perpetrator identifies a victim online and then orchestrates an opportunity to meet the victim in person without their knowledge. This demonstrates that interactions in the electronic space can have an adversarial effect in the physical-natural space between a perpetrator and a victim. As a result, many people who are victims of cyberstalking often fear for their physical well-being. Recent studies indicate that females are twice as likely as males to fear for their physical safety if they are a victim of cyberstalking (Maple, Short et al. 2012). Individuals who experience cyberstalking can often suffer from extreme psychological distress and this may have an adverse effect on their personal or professional lives, even in cases where the victim and the perpetrator never meet face-to-face (Strawhun, Adams et al. 2013). According to Short et al. (2014), cyberstalking may also have a detrimental impact on victims' everyday lives if they are forced to give up their hobbies, change jobs or abandon their personal relationships. Studies indicate that cyberstalking cultivates a long-term cycle of fear, the effects of which can vary wildly, as well as social isolation or physical or mental illness, particularly as victims have a tendency to avoid seeking help (Pereira and Matos 2015). Short et al. (2014) posit that such extreme implications are most common when the offender purposely involves the victim's loved ones in their manipulations and forces the victim to distance themselves from family and friends.

In many cases, the victim feels ashamed that they have been targeted and are embarrassed by the content of the communication from the perpetrator. As such, they are often reluctant to discuss the extent of the problem or in

doi:10.1016/j.tele.2016.08.016

several instances underestimate the significance of the problem itself. Many victims are also distressed by the apparent lack of adequate resources at their disposal to deal with cyberstalking and question the ability of the Police and internet service providers, the two parties responsible for tackling criminal activity online, to prevent harassment and provide counsel to those who have been targeted. Cyberstalking most certainly can have an adverse effect on the victim from a social, physical or psychological perspective; however, victims must endure a significant amount of harassment on behalf of the perpetrator before they can legitimately file charges. Due to the ambiguity surrounding cyberstalking from a legal standpoint, many victims may not receive the guidance or support that they need in dealing with unwanted attention. Thus, in order to improve existing protocols regarding the incidence of cyberstalking, it is necessary to analyse the behaviour of those targeted by online offenders and the services at their disposal to deal with the perpetrators.

In this study, we ask victims about their experiences and investigate the authorities to which incidents of online harassment and stalking are being reported. Particular focus is placed on analysing the perceived impact of intervention from these authorities and the role of Corporate Social Responsibility (CSR) in response to these anti-social offences. In the remaining part of this paper, a literature review is shared in Section 2 followed by the study's question and research scope in Section 3. In Section 4 we discuss our methodology. Analysis of results and discussion are then shared in Section 5 and Section 6 respectively. Study limitations are acknowledged in Section 7. Finally, we conclude our findings and recommendation in Section 8.

2. Background

2.1 Intervention and strategies against cyberstalking

Victims of cyberstalking adopt various defence strategies. These could include a confrontation with the perpetrator, asking for an intervention from a third-party, report to the Police or avoid/ignore contact (Miller 2012). Research also suggests that one of the most effective tactics utilises technology to block or shield communications from pursuers (Tokunaga and Aune 2015). Although, the response is usually associated with the type, duration and projected behaviour of a perpetrator in a given case.

Some victims favour offline training programmes to support them adapting an effective resolution (White and Carmody 2016). However, the benefit from participating in psychoeducational Internet safety interventions can be limited to increasing user knowledge without being significantly effective in changing their risky online behaviours (Mishna, Cook et al. 2010). Alternatively, new laws have emerged that consider cyberstalking to be a criminal offence. (Hazelwood and Koon-Magnin 2013)

Intervention and defence strategies against cyberstalking can be facilitated further by means of developing technology to automatically detect, classify, filter and consequently block unwanted messages (Ghasem, Frommholz et al. 2015, Frommholz, al-Khateeb et al. 2016). Research shows virtual agents have been proposed to provide advice and social support (al-Khateeb and Epiphaniou 2016).

2.2 Ethics and Corporate Social Responsibility (CSR)

Cyberstalking takes place in the cyberspace enabled by infrastructure offered by corporations such as Internet Service Providers and Mobile Operators. For these service providers to be a responsible member of the community, a self-regulatory code of conduct on a voluntary basis can be followed to mitigate cyberstalking (Smith and Steffgen 2013). A more consistent response is achievable when service providers communicate with law enforcement to avoid conflicting advice, and therefore confusion and stress to victims (Short and McMurray 2009).

Over the years, the concept of CSR emerged from a decision exclusively taken and controlled by executive managers to a more strategic component where a corporation policy in this regard can be supported by the United Nations Global Impact (UNGI) and the International Organisation for Standardization (ISO). For instance, it has been anticipated that ISO 26000:2010 will help organisations to contribute effectively towards sustainable development beyond their legal compliance, it is therefore an obligation to the public and larger society.

There is an ongoing discussion on what defines CSR (Murphy and Schlegelmilch 2013), but this is expected because it is also an umbrella term used for many other concepts including -but not limited to- ethics and equality at the work place. Ethics and CSR are frequently discussed together with some studies suggesting that ethics are applied within a company as part of their internal procedures while CSR is associated with external

doi:10.1016/j.tele.2016.08.016

entities. Matten and Moon (2008) argue that values change over time and this would continue to affect our perception and subjectivity as to what CSR is. However, at its core the meaning evolves around the consequences of business success on stakeholders and the environment within which businesses realise their activities and mission. CSR is implemented as policies and codes of conduct to demonstrate the corporation's willingness to increase the positive impact of its business towards the wider society. Therefore, ethics are bounded to CSR practices and have been described as one of the four main outlines; economic, legal, ethical and philanthropic (Carroll 1979).

Consequently, companies are also recognised for their Corporate Social Irresponsibility (CSI). Examples include unfair treatment of some of their employees, environmental damage (e.g. pollution) and low quality products with implication on their consumers. Jones, Bowd et al. (2009) explain with examples; it is irresponsible for a company to solely aim at developing a new technology and introduce it to the market, instead, an ethical CSR in this case is to adopt a policy stating that new technologies must be first tested and evaluated thoroughly to mitigate side-effects and any associated risks.

Further, Corporate Governance (CG) can play a major rule to shape CSR policies, Jamali, Safieddine et al. (2008) studied CG and CSR jointly and found that in practice the majority of managers utilise CG as a critical factor towards sustainable CSR.

3. Study questions and scope

This study forms part of the Electronic Communication Harassment Observation (ECHO) project that was launched in the UK to investigate and have a better understanding of cyberstalking, its impact, raise awareness among the population and to consequently contribute towards solutions for the community. As part of the second phase of ECHO, we move towards investigating the following research questions:

> *To what different authorities do people report incidents of cyberstalking? Do they find satisfactory response or intervention in return? And how can this be improved?*

The term cyberstalking in this context refers to online harassment or stalking. Examples of authorities in this study include law enforcement agencies such as the Police or otherwise any party with the ability to intervene including (but not limited to): Internet Service Providers (ISP) since they own and control the medium of communication, and owners of online platforms such as website moderators who have administrative privileges over the environment.

4. Methodology

4.1 Instruments and procedure

A mixed methodology approach was used in this study to provide added value by means of deeper and fuller answers in addition to quantitative data. Data collection took place by means of an online survey. The survey was made available and promoted through awareness seminars and Social Media (e.g. Twitter) with help from charities and national helplines in the UK such as the Network for Surviving Stalking (NSS). Access to the survey was given via an online link through the website of the University of Bedfordshire. To record quantitative data, participants were given multiple choice options or Likert-type scales where appropriate. Similarly, text/area boxes were used to capture qualitative data. The questions were developed iteratively by multidisciplinary researchers and professionals working in the area of cyberstalking. The number of participants answering a particular question could be less than the sample size for any given question since many questions were not compulsory due to the sensitivity of the subject.

Statistical test (*t*-test) was used to calculate the values of t-statistics (t-value), degree of freedom (df) and two-tailed probability (p-value) to determine if there was a significant difference between proportions. This helped to observe real difference (p-value is less than 0.05), or not (the p-value is equal to or more than 0.05), between the two populations and reported as: t(df)=t-value, p=p-value. The p-value is therefore a numerical value used to measure statistical significance.

Qualitative responses were thematically analysed using a phenomenological approach. Analysis was inductive: using the actual data to derive the structure. The findings were then critically analysed and discussed with arguments supported by expert opinion and literature to extend our understanding of the problem and to propose changes to the existing system to reform and enable better incident response.

doi:10.1016/j.tele.2016.08.016

4.2 Survey questions

To fully address our research questions with evidence-based discussion, self-identified victims were first asked to select and share feedback on the environment in which harassment incidents took place; this could have been a dating site, mobile text or work email. Such detail helped to identify relevant authorities and discuss their possible accountability and social responsibility. Besides, rate-of-occurrences, stalking behaviour was collected to understand which environments were exploited more often to investigate associated vulnerabilities and countermeasures. Participants were then asked to share a review of the key authorities they had reported harassment to (if any) and the follow up experience and consequent impact upon their case. Further, reasons for not reporting incidents were considered. Participants were also asked to share their perception of additional actions from relevant authorities that could have helped.

4.3 Ethics

The survey starts with a consent form containing information on the objectives of this study and assuring that data would be stored securely and analysed anonymously by a team of researchers. Participants were provided with contact information for further support, they were also given a chance to opt-out at any time should they decide to withdraw. The proposal for this study was approved by the University of Bedfordshire Ethics Committee.

5. Analysis of results

5.1 Sample description

The survey was conducted over three years between 2011 and 2014. During this period a total number of 305 responses were collected from which 274 are individuals who have experienced online harassment. The questionnaire captured demographic information which showed that 74% were females, 21.3% were males and the remaining preferred not to disclose their gender. They were aged 16-64 (Mean=36.5, Standard Deviation=11.8), and were regular users of the internet with 79% checking their emails 5 times or more daily.

5.2 Harassment rate-of-occurrences and possible correlation with the environment

The results show that we can distinguish between four different groups within the list of environments shown in Table 1.

Group1. This is where the highest rates of harassment incidents were reported. It includes *Personal webmail* (e.g. Gmail, Outlook …), *Mobile texts*, *Social Networks* (SN) (e.g. Facebook, Twitter and LinkedIn) and *Mobile phone calls*. *t*-test shows no significant difference between *Personal webmail* (63.5%) and *Mobile phone calls (54.3%)*; t(273)=1.408, p=.160.

Group 2. The second group includes *Physical environment;* it stands out with 40.8% of harassment incidents. This value is statistically different from Group 1 (*mobile phone calls*: 54.3%); t(273)=2.314, p=.021. Likewise, there is a significant variation in the number of stalking incidents between the *Physical environment* (4.7%) and Group 1 (*Mobile phone calls*: 10.9%); t(273)=2.631, p=.009. Since there is currently no legal definition for online stalking in the UK, our study comes to an agreement with previous research (Mullen, Pathé et al. 2000) to suggest a combination of online targeted harassment with ten or more occurrences happening over a period of four weeks as an effective means to identify this malicious behaviour.

doi:10.1016/j.tele.2016.08.016

Table 1 – Environment and the frequency of harassing incidents, participants were asked to select all that apply, n=274. The list is sorted by the number of harassments reported.

Environment	*Harassment %*	*Over a period of 4 weeks or more %*	*On 10 or more occasions %*	*Stalking %*
Personal webmail	63.5	18.6	40.5	12
Mobile texts	57.2	26.6	32.1	11.3
Social Networks	54.3	25.5	32.8	12
Mobile phone calls	54.3	18.9	31.7	10.9
Physical environment	40.8	8.3	16.7	4.7
Work email	29.5	7.6	16.7	4.3
Online Discussion Boards	27.3	8	14.2	3.2
Instant Messaging services	26.2	8.3	11.6	4.7
Blogs	22.6	5.4	15.6	2.5
Online dating sites	13.5	1.8	3.2	0
Chatrooms	12.7	2.5	8	1.4
Other online games	6.2	1.4	3.6	0.7
MMORPG	5.1	0.7	2.1	0.3

Group 3. This group stands out with statistical difference when compared to Group 2, it includes *Work email*, *Online Discussion Boards* (Also known as Bulletins or Forums), *Instant Messaging (IM) services* (e.g. WhatsApp, Skype and Yahoo! Messenger) and finally *Blogs*. *t*-test shows no significant difference between *Work mail* (29.5%) and *Blogs* (22.6%); t(273)=1.59, p=.113.

Group 4. This last group includes the remaining environments in Table 1, they had the least number of reported incidents. *t*-test shows significant difference between Group 3 (*Blogs: 22.6%)* and Group 4 starting with *Online dating sites* (13.5%), t(273)=2.536, p=.012.

Online games including those titled as Massively Multiplayer Online Role-Playing Games (MMORPG) have the least incidents reported but findings uncover an evidence of stalking which is interesting considering the type of activity designed for such platforms. Our results also suggest a clear correlation between the number of users of a particular environment and the amount of reported harassment within our sample. With regards to our scope, the objective of this investigation is to clearly highlight most exploited environments to identify relevant authorities as discussed earlier.

5.3 Follow-up experience and impact after reporting harassment

Participants were asked to rate and comment on their experience after the incident was reported to the relevant authorities, the results are shown in Table 2. As an overall comparison, the positive impact is statistically not significant across all four authorities. However, investigating the negative impact shows significant difference between Mobile Operators (MO) and the Police t(255)=1.975, p=.049, and between MO and website/chat admins t(163)=2.533, p=.012, in favour of MO in both cases.

Table 2 – Perceived impact on the case after reporting harassment to authorities such as the Police, MO, ISP or website/online Chat-room Administrators.

Outcome	*Police %*	*MO. %*	*ISP %*	*Website admin %*
Made things a lot worse	15	6.1	13.3	17.6
Made things slightly worse	3.1	3	4.4	5.8
Had no effect	51.8	57.7	66.6	57.3
Made things slightly better	19.3	19.5	13.3	16.1
Made things a lot better	10.6	13.4	2.2	2.9
	(n=160)	*(n=97)*	*(n=45)*	*(n=68)*

Furthermore, 41.6% of our sample (114, n=274) did not report their case to the Police, and Table 3 shows how many individuals did not report their case to the relevant service provider. Our findings suggest that the proportion of those who did not know they could report it is significantly more than those who knew but choose not to at the time – MO: t(115)=3.082, p=.003; ISP: t(143)=9.977, p<.001; website/chat admin: t(94)=4.118, p<.001.

doi:10.1016/j.tele.2016.08.016

Table 3 – Number of individuals who have NOT reported the incident to parties other than the Police and key reason they selected to explain why, n is the total number of participants with an incident relevant to that particular service provider.

Outcome	*MO %*	*ISP %*	*Website admin %*
Did not know/think about	63.7	81.9	69.4
Knew/thought about but did not use	36.2	18	30.5
	(n=116)	*(n=144)*	*(n=95)*
Did not report (in total)	54.4% (116)	*76.1% (144)*	*58.2% (95)*
	(n=213)	*(n=189)*	*(n=163)*

To explain the rationale behind these numbers participants were asked to share their experience in further details.

Experience with the Police

Four overarching themes emerged: lack of evidence (harasser anonymity and forensic evidence); hesitation to report (fear of escalation and emotional reasons), variation in Police responses (civil matter, lack of support, reassuring, warning the harasser, lack of update) and breaking restraining orders and injunctions.

The *Lack of evidence* theme was mainly due to the anonymity of the harasser; because most of the perpetrators utilised online communication services with virtual IDs which were not linked to a known person: "*Police stopped direct contact, but now anonymous*" (Participant 101); this was perceived by some participants to have prevented the Police from taking further action since no party could be identified for investigation: "*I asked to lay a charge of cyberstalking against person(s) unknown, but they don't seem to have done anything about it*" (58). Furthermore, it was critical that evidence exist to support the case which was quite challenging to both participants and Police due to reasons such as the dynamic nature of online communication and the victims lack of technical expertise to preserve admissible digital evidence. As such, many participants reported this requirement frequently using terms of needing evidence, difficulty to get evidence or insufficient evidence to qualify stalking behaviour "*… Police need evidence*" (158) "*Police said I couldn't prove harassment on phone. They were right. I still can't*" (72).

In the *Hesitation to report* theme many participants expressed that victims did not report to the Police because they fear escalating the problem "*Contacted Police then saw another comment left and decided not to go further for fear of escalation of behaviour on the behalf of the stalker*" (24) Other participants did not report to the Police due to an emotional reason such as guilt and/or sympathy: "*Police involvement could greatly affect their ability to get a job (CRB check), so was a last resort as didn't want the guilt of potentially ruining somebody's career, even though it was serious abuse*" (60)

The *Variations in Police responses* theme highlighted that participants who reported an incident to the Police received different responses. For instance, many were told it was a civil matter and this was accompanied by a perceived lack of support expressed by many participants giving very short comments about the Police not being interested, with relatively few participants who reported being reassured or an action taken by the Police to stop harassment. "*… I was (sic) received a death threat by phone. […] the Police were very reassuring and I felt much safer as a result*" (121). Many participants complained of a lack of update or a delay in communication from the Police: "*Police who asked for evidence. Once sent, they stopped communicating with me.*" (15).
In the *Breaking restraining orders* theme participants suggested that despite the action taken by the Police in some cases this was commonly followed by the harassers breaching the restraining orders or injunctions issued. "*Reported to Police and got a restraining order which he has repeatedly flouted*" (184).

Experience with Mobile Operators

Four overarching themes emerged: changing phone number; blocking harasser number; limited actions by MO and unknown Caller ID.

The *Changing phone number* theme highlighted that the majority of participants reported they had changed their phone number to avoid the malicious communication and this helped in stopping the harassment as a positive outcome in some cases. However, some stalkers were very persistent: "*I have changed my number several times with in a six-month period and yet it still continues*" (161). Some participants considered getting a silent number, this is a number that is intentionally unlisted in telephone books (and their likes) for privacy reasons: "*disconnected phone and got new silent number"* (63). Nonetheless, there were perceived challenges in

doi:10.1016/j.tele.2016.08.016

changing the phone number such as the difficulty in changing a number they have been using for years as the only measure given to them to mitigate the problem or the extra charges they had to pay to MO: *"... offered to change my mobile number but would have charged me £30"* (287)

In the *Limited actions by MO* theme participants consistently suggested there was no action taken by the MO to help. The suggested solutions by the MO relied mostly on victims focusing on ignoring calls, advice to change phone number or disapproval of requests to block certain numbers: *"I asked […] to block a number of an ex boyfriend who wouldn't stop calling me but they said they couldn't do anything unless I changed my number"* (121).

The *Blocking harasser number* theme emerged as individual actions taken by victims secondary to perceived lack of support from the MO. This led many participants to look for other ways such as attempting to block specific numbers identified as belonging to the perpetrator or blocking all withheld numbers. These options were actioned solely by the participants since many have reported that the MO refused to block numbers: "*As I'm on Pay As You Go and not contract, […] said that blocking numbers wasn't an option. I can add numbers to reject list but this still means my phone buzzes and I get the voicemail symbol up for three days unless I pay to call and delete each message*" (174).

The *Unknown caller ID* theme was a challenge to many participants who specifically shared their experience with Unknown Caller IDs since they are difficult to trace and investigate making it a source helplessness: "*did not do so [report] because most of the worst harassment I did not know where it was coming from*" (157).

Experience with ISPs

Two themes emerged: removing content and policy related issues. It is important to highlight that comments were found to cover both ISP and web site/service hosting companies.
With regards to the *Removing content* theme, many respondents stated that companies were taking down harassing content: "*Reported to […] and hateful blogs were removed*" (39), but this was not always the case because some participants were faced with rejection: "*reported to [global companies] both American Companies they refused (sic) to take content down*" (24). However, no participant reported the same for ISPs, and since their services focus on infrastructure rather than data management "*They claim they are only provides and not responsible for content*" (162).

The *Policy related issues* theme reflected on issues such as lack of systematic action or advice to their customers on such cases. Participants felt there was no policy or training in place to deal with their inquiries: "*[…] were useless; I explained the situation to them and they seemed to have no experience. i was owrried (sic) he was intercepting my emails, they just repeatedly cut off my service provision […]; I had to go to the CEO in the end and then they sorted it out*" (293). At times, the solution given was not efficient such as bulk blocking emails coming from the same provider which was mostly inconvenient to victims because it could result in blocking other people not involved in harassment.

Experience with website/chat administrators

Three themes emerged: lack of action, removing content and reporting system. In the *Lack of action* theme participants highlighted that some websites tended to take no action or do not reply to their communication: "*Sent several messages to […] administrators but did not receive any reply*" (165).Consequently, the *Removing content* theme was identified when a group of participants shared that persistent attempts in reporting eventually lead to action which was mainly limited to removing the offensive content "*The chatroom moderator removed the offending post after several requests*" (137); although this was challenged by the harassers ability to easily create new account and continue to post: "*The harrasor (sic) kept changing email addresses, opening and closing accounts…*" (30). The *Reporting system* theme was identified in response to where participants frequently attempted to report their cases but they perceived limitations in reporting systems when they were faced by difficulties in reporting or non- practical advice received at the end of the process.: "*[administrators] were uncontactable - I followed their (sic) rubbish report abuse system but only got to the change password options*" (200).

5.4 Perceptions of actions that could have helped if made available

When asked what other actions could have helped, the majority of participants supported the idea of an independent third-party intervening with the harasser on their behalf with no significant difference from those

doi:10.1016/j.tele.2016.08.016

who have asked for other Police action; t(273)=1.375, p=.170 but significant difference from the rest as shown in Table 4. Intervention by the employer was the least favourite which could be due to a number of reasons. For instance, people could worry about the negative impact upon their career or reputation at work (Short, Linford et al. 2014). Harassment in the sample of this study was not mainly linked to the work place or participants might have thought that intervention is the responsibility of law enforcement.

Table 4 – Participants rated actions that could have helped if made available, n=274.

Action	*Participants %*
Notification to your harasser/stalker by an independent anti-stalking organisation	66.4
Other Police actions	57.2
Intervention from network providers	51
Other	28.4
Intervention by your employer	11.3

Three themes emerged when responses from those selecting "Other" were analysed, namely: emotional support, technical solutions and more intervention by authorities. Many participants have asked for more emotional and educational support to be provided seeking more understanding from other people, especially their friends: "*friends believing me would be helpful, but many don't*" (182); and to help them (the victims) to realise the problem better: "*more information in the public sphere so that I knew that it was common what is happening to me*" (43). Responses shared wishes for the technology to be actively deployed in defence e.g. to enforce traceable communication and link SIM cards to a physical identity to support investigations: "*sim cards should only be activated after registration*" (213). More intervention was mainly expressed by means of blocking perpetrators: "*The harasser being blocked by their internet service provider*" (137); and a bigger role to be played by the Police in particular: "*The Police utilising any of the many legal tools that were available in this case*" (141).

6. Discussion

Females have reported the majority of incidents in this study, a similar ratio outcome can be observed in previous surveys conducted in the US (Baum, Catalano et al. 2009) and the UK (Maple, Short et al. 2012). An analysis of three surveys on youth Internet safety has also found an increasing proportion of female victims; from 48% in 2000 to 69% in 2010 (Jones, Mitchell et al. 2013). It is possible that females were more engaged with surveys because they experience higher levels of stress compared to males (Maple, Short et al. 2012). In general, gender and sexual orientation of individuals can be factors to increase targeted online harassment (Mitchell, Ybarra et al. 2014). Having said that, a study by Finn (2004) shows that men were as likely to experience e-mail harassment as women.

From an Incident Response perspective (Casey 2011), it is critical to define the environment where cyberstalking events are taking place, as this helps to plan for relevant/optimal countermeasures put in place. In particular, threat modelling and risk assessment could help in this process as there is limited information published in the public domain on the necessity of identifying threats and vulnerabilities in cyberstalking. The majority of incidents manifested on what has been described as a personal communication channel (e.g. personal email, mobile text) rather than public venues such as discussion forums, blogs and chat rooms. This does not necessarily mean harassers are successful at collecting personal information about their targets. We believe the majority of incidents arise from those already familiar with their targets as confirmed by participants' answers to our open-ended questions. These could include extended family members, friends, colleagues and ex-partners. Heinrich (2015) examined the victim offender relationship of 1,040 college students and reported ex-intimate partners as the most popular theme in the case of cyberstalking while strangers were more popular in offline incidents.

Services such as personal webmail, mobile text/calls and social networking are usually offered by cross-border (large) corporations with infrastructure and partnerships across the globe, often served over pervasive networks (e.g. the Cloud). We argue on this distinctive characteristic to encourage a reasonable level of liability to these companies to enable a safer environment to their customers. They can develop strong internal policies, procedures and schemes to support victims of cyberstalking and align those with their internal security policy programme in either tactical or operational level. Our results indicate a potential market advantage and positive customer satisfaction for companies implementing means of intervention as part of their operation. This

doi:10.1016/j.tele.2016.08.016

initiative can be associated with, and encouraged by, the company's own CSR and strategic planning towards achieving competitive advantage (Wagner III and Hollenbeck 2014). It should be realised that service providers might be the only independent party having the required privilege and accessibility to evidence what has been communicated to their customers, or provide efficient means to block unwanted communications. Additionally, unlike law enforcements who have to go through formalities when investigating a case outside their local borders, companies can help to mitigate or resist anti-social behaviour worldwide via their own policies. Furthermore, companies' regulations can be re-visited and updated relatively quickly compared to legislations.

Currently and for objectives related to the competitive market advantage, many operators (e.g. Sky) have recognised the need to support their clients with free protection against malware, or backup solutions to store and recover personal data. For the same reason, financial institutions offering online services (e.g. Barclays) give away free Internet security products. Likewise, another way competitive advantage could be maintained is with the implementation of countermeasures against online harassment and stalking.

To describe the current situation, our findings show no systematic response and very limited help given to victims by Mobile Operators and ISPs. Examples include but are not limited to: lack of professional advice and experience on the matter; and implementing charges on victims for measures they had to take to protect themselves. At this point we need to emphasise that the externality factor states that privacy violations of the clients' data do not constitute a significant impact upon the company's security decision making which can partially explain the little evidence of positive interventions.

ISPs tend to argue on the boundaries of their responsibility because their work is more focused on providing infrastructure and will not monitor content without a request by Law Enforcement, usually supported by a warrant from a Court of Law (Trepel 2007). Additionally, the large amount of data crossing an ISPs infrastructure makes it impractical to conduct routine investigations. Even when these investigations are feasible, several concerns must be tackled around privacy and data protection laws (Finn, Wright et al. 2013). Also, our study shows random responses were given to individuals reporting harassment which could suggest a lack of staff training and more importantly the unavailability of a policy to govern responses to this type of threat. To showcase examples of good responses we suggest explicit advice on who to contact for help (e.g. National Stalking Helpline). Since many ISPs offer additional web services and emails, an example of a good response could be to confirm whether a reported harassment comes from a fraudulent account or not. Nonetheless, we also want to raise awareness on the possibility of implementing strict Acceptable Use Policies (AUP) when it comes to online harassment and stalking. Examples could be appropriate restrictions to users systematically engaging in such behaviours such as termination of their contracts, rejection of service or refusal of access to specific resources. Although more research is needed to examine the effectiveness of this approach, companies already run different check-ups on the financial state of their customers prior to approving their contract. We project this would encourage people to have a healthier behaviour online following a companies' initiative to incorporate these AUPs as part of their CSR.

One of the interesting findings of this study is the situation where a victim of an anti-social behaviour chooses to avoid Law Enforcement in favour of a private resolution to the case by a third-party (e.g. service providers). Reasons include a victims' willingness to protect the offender from being arrested or served a formal warning by the Police. Such cases would typically involve a friend, family member or ex-partner as the offender (Barnes and Short 2015). This shows that the personal relationship between the victim and the harasser should be taken into account as part of any mitigation procedure. As such, the reasoning behind sending unwanted messages could be an attempt to get closer to the target rather than causing intentional harm. However, other reasons include fear of escalation, guilt/sympathy and self-blaming as our findings suggest.

A considerable number of participants reported a negative impact on their cases after they were reported to the Police. While an early survey of stalking victims in the UK reported 41% of their sample were unhappy with the way the Police had handled their cases and the inadequacy of the law at that time (Sheridan, Davies et al. 2001), our study shows the Police's inability to help was due to lack of evidence or the anonymity of the perpetrator. It should be noted that low/negative rating given to the Police to-a-degree could be influenced by the fact that many participants are still living the consequences of unresolved cases e.g. Police investigation have not concluded. Having said that, analysis of reported incidents in our sample shows the Police were people's first-point-of-contact which is consistent with findings from other surveys (Fazio and Galeazzi 2004, Kamphuis, Galeazzi et al. 2005). Therefore, it is essential to give local Police officers sufficient training on the subject.

The vast majority of participants (66%) supported the idea of a third-party intervention to contact harassers/stalkers on their behalf followed by a second popular opinion that further actions should be taken by

doi:10.1016/j.tele.2016.08.016

the Police. However, very few (11.3%) were happy to accept an intervention by their employer. As such, victims want to illuminate the impact of cyberstalking on their lives, thus while they are keen for a third-party to intervene and help, they are protective when it comes to affecting their own workplace and career.

7. Limitations

In common with previous works cited earlier, this study utilised non-probability based sampling. Hence, results can suggest hypotheses for further study but generalisation to the entire population of cyberstalking victims is not possible. Further, this is a self-report survey, and so, there can be social desirability bias, participants may exaggerate symptoms, or likewise, they may underestimate the severity or feel embarrassed to share private details. Therefore, open questions were used to allow respondents to expand upon their answers.
It should also be realised that an unknown number of individuals may have chosen not to define themselves as victims of cyberstalking, or were not willing to share their experience, or had not seen this survey. Moreover, response errors are possible due to the frailty of memory, not everyone keeps notes. As such, it cannot be assumed that participants included in this survey were representative of all stalking victims in the population.

Throughout this paper, responses from participants were treated as genuine record of incidents, and so, terms such as 'Claimed' and 'Alleged' could have been omitted in some places.

The response-rate was difficult to calculate because it is not possible to determine the number of people who have received, opened or read invitations to their social media accounts or emails.

Nevertheless, due to different definitions used in the literature for online harassment and stalking, the process of comparing existing works seems to be an arduous task. We argue that the vocabulary used for these terms must be unified so as to simplify the process of identifying conflicting relationships and commonalities between them.

8. Conclusions and recommendations

A significant number of participants who have been identified as victims of online harassment and stalking were unaware or did not think about reporting the incidents/offences to relevant service providers. User awareness should be raised to correlate between the exploited environment and the potential liability of the owner (service provider or service manager) to take action.

The majority of events took place within communication channels, most of which are usually owned and controlled by large, cross-border international companies providing mobile services, webmail or social networking. Survey results from those who have reported incidents to such companies (e.g. Mobile Operators and ISPs) demonstrate a very low level of support given to these victims. In some cases, charges were enforced such as where users had to pay a fee to change their number. We describe this lack of ability to support victims of cyberstalking as a Corporate Social Irresponsibility (CSI) (Jones, Bowd et al. 2009), and urge on the necessity to raise the expectations of customers together with advising such corporations to consider improving their competitive advantage in the market through better internal policies and AUPs. Further, Service Providers could implement Corporate Governance (CG) protocols to enforce and verify that effective measures are in place to mitigate harassment. This is very important because Board Oversight and a lack of governance was the key reason for many unethical and - at times- illegal activities within businesses (Murphy and Schlegelmilch 2013).

In many countries such as the UK, each resident has a credit history and credit score that is analysed before financial contracts are approved. While the idea of applying a similar system nationally to penalise perpetrators could be appealing at first instance, we realise the difficulty –at least for the time being- to have this implemented. Therefore, our recommendation is to consider and encourage having a strong AUP for each company as part of their own strategy and Corporate Social Responsibility.

The results on reporting harassment to website/chat administrators showed no or very little help was received compared to intervention by other authorities. Cases of each website could be unique but considering the minimal privileges administrators have to run a service, they should still be able to block flagged accounts and help generate evidence when required. For a website to provide a user-friendly environment, mechanisms to report unwanted content must be coded efficiently and made available to all users supported by clear policies. A possible contribution in this area could be a framework to help website owners building harassment-aware applications.

doi:10.1016/j.tele.2016.08.016

The first-point-of-contact and most popular authority to whom incidents were reported was the Police. Key issues causing negative experiences in this case was a lack of evidence. There is a need to explore how the Police can provide further help to guide end-users towards building admissible evidence. A web or mobile application to intercept unwanted messages could be a reasonable step in response to this difficulty given that end users are not technology gurus and would need a user-friendly method to support them. Frommholz, al-Khateeb et al. (2016) proposed a framework to address this requirement but such research is still in its infancy. Finally, the majority of participants have clearly preferred third-party intervention on their behalf to mitigate risks associated with cyberstalking. An independent specialist anti-stalking organisation was preferred to act on their behalf followed by the Police and network providers.

References

al-Khateeb, H. M. and G. Epiphaniou (2016). "How technology can mitigate and counteract cyber-stalking and online grooming." Computer Fraud & Security **2016**(1): 14-18. doi:10.1016/S1361-3723(16)30008-2.

Barnes, J. and E. Short (2015). Who Stalks and Why. A practical Guide to Coping with Cyberstalking. NCCR. The National Centre for Cyberstalking Research, Andrews UK Limited.

Baum, K., S. Catalano, M. Rand and K. Rose (2009). "Stalking Victimization in the United States. US Department of Justice Bureau of Justice Statistics." NCJ **224527**.

Carroll, A. B. (1979). "A three-dimensional conceptual model of corporate performance." Academy of management review **4**(4): 497-505.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet, Academic press.

CPS. (1997). "Stalking and Harassment." from http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/.

Davis, K. E., A. L. Coker and M. Sanderson (2002). "Physical and mental health effects of being stalked for men and women." Violence and Victims **17**(4): 429-443.

Dreßing, H., J. Bailer, A. Anders, H. Wagner and C. Gallas (2014). "Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims." Cyberpsychology, Behavior And Social Networking **17**(2): 61-67.

Fazio, L. D. and G. M. Galeazzi (2004). "Women Victims of Stalking and Helping Professions: Recognition and Intervention in the Italian Context " Faculty of Criminal Justice, Univeristy of Maribor, Slovenia.

Finn, J. (2004). "A survey of online harassment at a university campus." Journal of Interpersonal violence **19**(4): 468-483.

Finn, R. L., D. Wright and M. Friedewald (2013). Seven types of privacy. European data protection: coming of age, Springer**:** 3-32.

Frommholz, I., H. M. al-Khateeb, M. Potthast, Z. Ghasem, M. Shukla and E. Short (2016). "On Textual Analysis and Machine Learning for Cyberstalking Detection." Datenbank-Spektrum, 16(2), pp.127-135, ISSN 1618-2162. doi:10.1007/s13222-016-0221-x

Ghasem, Z., I. Frommholz and C. Maple (2015). A Machine Learning Framework to Detect And Document Text-based Cyberstalking. in Proceedings Information Retrieval Workshop at Lernen-Wissen-Adaptivität (LWA 2015).

Hazelwood, S. D. and S. Koon-Magnin (2013). "Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis." International Journal of Cyber Criminology **7**(2): 155.

Heinrich, P. A. (2015). "Generation iStalk: an Examination of the prior relationship between victims of stalking and offenders."

doi:10.1016/j.tele.2016.08.016

Home Office. (2012). "Circular: a change to the Protection from Harassment Act 1997." from https://www.gov.uk/government/publications/a-change-to-the-protection-from-harassment-act-1997-introduction-of-two-new-specific-offences-of-stalking.

Jamali, D., A. M. Safieddine and M. Rabbath (2008). "Corporate governance and corporate social responsibility synergies and interrelationships." Corporate Governance: An International Review **16**(5): 443-459.

Jones, B., R. Bowd and R. Tench (2009). "Corporate irresponsibility and corporate social responsibility: competing realities." Social Responsibility Journal **5**(3): 300-310.

Jones, L. M., K. J. Mitchell and D. Finkelhor (2013). "Online harassment in context: Trends from three Youth Internet Safety Surveys (2000, 2005, 2010)." Psychology of Violence **3**(1): 53.

Kamphuis, J. H., G. M. Galeazzi, L. De Fazio, P. M. Emmelkamp, F. Farnham, A. Groenen, D. James and G. Vervaeke (2005). "Stalking—perceptions and attitudes amongst helping professions. An EU cross-national comparison." Clinical psychology & psychotherapy **12**(3): 215-225.

Kropp, P. R., S. D. Hart, D. R. Lyon and J. E. Storey (2011). "The development and validation of the guidelines for stalking assessment and management." Behavioral sciences & the law **29**(2): 302-316.

Maass, A., M. Cadinu and S. Galdi (2013). "Sexual harassment: Motivations and consequences." The Sage handbook of gender and psychology: 341-358.

Maple, C., E. Short, A. Brown, C. Bryden and M. Salter (2012). "Cyberstalking in the UK: Analysis and Recommendations." International Journal of Distributed Systems and Technologies (IJDST) **3**(4): 34-51.

Matten, D. and J. Moon (2008). ""Implicit" and "explicit" CSR: a conceptual framework for a comparative understanding of corporate social responsibility." Academy of management Review **33**(2): 404-424.

Miller, L. (2012). "Stalking: Patterns, motives, and intervention strategies." Aggression and Violent Behavior **17**(6): 495-506.

Mishna, F., C. Cook, M. Saini, M.-J. Wu and R. MacFadden (2010). "Interventions to prevent and reduce cyber abuse of youth: A systematic review." Research on Social Work Practice.

Mitchell, K. J., M. L. Ybarra and J. D. Korchmaros (2014). "Sexual harassment among adolescents of different sexual orientations and gender identities." Child abuse & neglect **38**(2): 280-295.

Mullen, P. E., M. Pathé and R. Purcell (2000). Stalkers and their victims, Cambridge University Press.

Mullen, P. E., M. Pathé and R. Purcell (2004). "Stalking: Defining and prosecuting a new category of offending." International Journal of Law and Psychiatry(27): 157-169.

Murphy, P. E. and B. B. Schlegelmilch (2013). "Corporate social responsibility and corporate social irresponsibility: Introduction to a special topic section." Journal of Business Research **66**(10): 1807-1813.

ONS. (2015). "Internet Access - Households and Individuals " Retrieved 11-2-2016, from http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/2015/index.html.

Path, M. and P. E. Mullen (1997). "The impact of stalkers on their victims." The British Journal of Psychiatry **170**(1): 12-17.

Pathe, M. T., P. E. Mullen and R. Purcell (2000). "Same-gender stalking." J Am Acad Psychiatry Law **28**(2): 191-197.

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

doi:10.1016/j.tele.2016.08.016

Pittaro, M. L. (2007). "Cyber stalking: An analysis of online harassment and intimidation." International Journal of Cyber Criminology **1**(2): 180-197.

Sheridan, L., G. Davies and J. Boon (2001). "The course and nature of stalking: A victim perspective." The Howard Journal of Criminal Justice **40**(3): 215-234.

Short, E., S. Linford, J. M. Wheatcroft and C. Maple (2014). "The Impact of Cyberstalking: The Lived Experience-A Thematic Analysis." Stud Health Technol Inform **199**: 133-137.

Short, E. and I. McMurray (2009). "Mobile Phone Harassment: An Exploration of Student's Perceptions of Intrusive Texting Behavior."

Smith, P. K. and G. Steffgen (2013). Cyberbullying through the new media: Findings from an international network, Psychology Press.

Strawhun, J., N. Adams and M. T. Huss (2013). "The assessment of cyberstalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse." Violence and victims **28**(4): 715-730.

Tokunaga, R. S. and K. S. Aune (2015). "Cyber-Defense A Taxonomy of Tactics for Managing Cyberstalking." Journal of interpersonal violence: 0886260515589564.

Trepel, S. (2007). "Digital Searches, General Warrants, and the case for the Courts." Yale JL & Tech. **10**: 120.

Wagner III, J. A. and J. R. Hollenbeck (2014). Organizational behavior: Securing competitive advantage, Routledge.

White, W. E. and D. Carmody (2016). "Preventing Online Victimization College Students' Views on Intervention and Prevention." Journal of Interpersonal Violence: 0886260515625501.

WHO (1992). The ICD-10 classification of mental and behavioural disorders: clinical descriptions and diagnostic guidelines, Geneva: World Health Organization.

doi:10.1016/j.tele.2016.08.016