Millman, C., Winder, B. & Griffiths, M.D. (2017). UK-based police officers' perceptions of, and role in investigating, cyber-harassment as a crime. *International Journal of Technoethics,* 8, 87-102.

INTRODUCTION

Cyber-harassment is a criminal offence in the UK and victims can report instances to the police. The role of police officers is to investigate the crime and report their findings to the Crown Prosecution Service (CPS) who ultimately decide whether a case proceeds to court. Police officers' attitudes towards cyber-harassment play a central role in how they interact with victims and how they conduct criminal investigations. Victim accounts paint a bleak picture of the inability of police officers in tackling cyber-harassment (Burgess & Baker, 2002; Finn, 2004; Griffiths, 1999). To date, there is no empirical research focusing on police officers' attitudes towards cyber-harassment in the UK. This paper addresses this gap by examining how these crimes are investigated and issues and/or barriers faced by officers. Gaining insight into these issues helps to inform how individuals can protected from the misuse of technology, thereby contributing to the field of technology ethics.

The *Protection from Harassment Act (1997)* (*PfHA*) and the *Protection of Freedoms Act (2012)* (*PoFA*) can be used to prosecute perpetrators in the UK. Whilst broad enough to allow for the prosecution of perpetrators of cyber-harassment, the *PfHA* does not define cyber-harassment which results in ambiguity (Bocij, Griffiths & McFarlane, 2002). To address this, some cyber-harassing behaviors are stipulated in the more recent *PoFA* (including monitoring via the Internet, publishing material about someone else and identity theft). Whilst neither Act provides protection against unidentifiable perpetrators or those who live outside the UK (Salter & Bryden, 2009), they are the only legislative tools that can be used in the UK.

Despite cyber-harassment being a criminal offence, little empirical research has included police officers. However, Kamphuis, Emmelkamp and deVries (2004) investigated police officers' responses in a vignette study examining stalking behaviors (mainly offline) that varied in severity, frequency, and intrusiveness. They reported that police officers normalized stalking behaviors and the authors attributed this to desensitization resulting from exposure to criminal activity. Whilst officers from four countries participated, the authors reported that UK-based officers were least likely to engage in victim-blame. UK-based officers were also most likely to state that responding to stalking incidents was part of their job. The results suggest that UK-based officers may be sympathetic towards victims of cyber-harassment and be likely to take victims' reports seriously.

In another study, 12 Canadian police officers were interviewed about their perceptions and response to cyber-bullying (Broll & Huey, 2014). Officers did not perceive cyber-bullying as criminal per se but reported that if the perpetrator's behavior became threatening, they would respond to the behavior as a criminal matter. Police officers felt cyber-bullying was best tackled through education about Internet etiquette and online safety. However, it is unclear whether the cases dealt with met legal definitions cyber-harassment or whether participants minimized the behaviors involved.

Whilst cyber-harassment can have a significant detrimental impact on victims (e.g., Dreβing et al., 2014; Sinclair eta al., 2012; Short, Guppy, Hart & Barnes, 2015), few report harassment (offline or online) to the police (Budd & Mattinson, 2000; Finn, 2004; Fremouw, Westrup & Pennypacker, 1997; Tjaden & Thoennes, 1998). One reason is dissatisfaction with action taken with reports that police officers refuse or are powerless to help, or minimize the extent or impact of harassment. When action is taken (e.g., warnings, arrests, restraining orders etc.), it is often considered to be ineffective (Blaauw, Winkel, Arensman, Sheridan & Freeve, 2002; Burgess & Baker, 2002; Draucker, 1999; Finn, 2004; Griffiths, 1999; Morris,

Anderson & Murray, 2002; Roberts & Dziegielewski, 1996; Tjaden & Thoenes, 1998). However, much of this evidence is outdated and attitudes and understanding towards online behavior may have changed over the last decade. Consequently, there is a need to better understand police officers' perceptions of cyber-harassment and explore barriers they encounter when dealing with such cases.

One barrier may be that cases are dismissed due to insufficient evidence which reinforces the invulnerability of perpetrators. Cyber-forensics involves the scrutiny of hard discs on computers/digital devices, searching for 'digital footprints' to uncover a perpetrator's actions (Kaur, Kaur & Khurana, 2016). Cyber-forensic methods ultimately lead to a specific computer/device and not a person who can be prosecuted (Bocij, 2004; Griffiths, Rogers & Sparrow, 1998). Benefits of cyber-forensic measures may include making it easier to gather evidence, establishing burden of proof, and tracing perpetrators who attempt to remain anonymous (Salter & Bryden, 2009; Wall, 1998). However, cyber-forensics places high demand on resources (i.e., time, money, and technology) that may detrimentally impact on apprehending perpetrators. Furthermore, perpetrators of cyber-crime are becoming more adept at utilizing anti-forensic measures as technology advances (Yeboah-Boateng & Akwa-Bonsu, 2016).

One potential solution to combat cyber-harassment is for Internet users to utilize self-protective strategies that minimize their vulnerability. Whilst avoiding online spaces may infringe on the right to use the Internet (Bocij, 2004), such strategies are regularly used offline (Basu & Jones, 2007). 'Blocking' contact from potential perpetrators is a form of cyber-ostracism that may also be an effective strategy as it may regulate the perpetrator's behavior by invoking shame (Wall & Williams, 2007). However, the effectiveness of 'blocking' assumes that a sense of community exists in the online spaces used by perpetrators and that perpetrators are motivated to remain included these online communities.

Furthermore, ‘blocking’ may simply encourage perpetrators to find other means of communication (Salter & Bryden, 2009). For example, online harassment may be forced offline to satisfy the perpetrator’s obsession with their target. Whilst individuals can adopt protective strategies to minimize exposure to cyber-harassment, such strategies are unlikely to be effective in all cases.

To summarize, cyber-harassment is a criminal offence within the UK and when victims report the crime, they are often dissatisfied with how their case is dealt with. To date, there is little evidence about the views and attitudes of UK-based officers’ regarding cyber-harassment despite their gatekeeping role in the prosecution of cases. The objectives of the present study were to explore police officers’ perceptions of cyber-harassment and in particular, their perceptions of victims; to explore how police officers perceive their role in supporting and protecting individuals; and to evaluate the support given to victims.

METHOD

Participants

Eight self-selected UK-based police officers volunteered to participate in the present study, comprising one female and seven males aged between 26 and 55 years (M = 38 years; SD = 10 years). Participants had an average of 14.1 years of service (ranging from 2 to 29 years; SD = 9.6 years). Due to the hard-to-reach nature of the target population, snowball sampling was a convenient sampling strategy with initial contact being made with key personnel in police departments involved in cyber-crime. Participants worked in a range of police departments (including the Criminal Investigation Department, school liaison, and community), and all reported having been exposed to victims of cyber-harassment as part of

their job (via murder investigations, school-based cyber-bullying, responses to domestic violence, etc.).

Measures

Semi-structured interviews were conducted face-to-face (n=6) or via the telephone (n=2) to maximize participation given the difficulties in accessing the cohort. The interview schedule was devised following a literature review of the key issues in combating cyber-harassment. Specifically, to meet the study objectives, the schedule addressed perceptions of cyber-harassment, officers' role in dealing with cases, and exploring how individuals can be protected from cyber-harassment. Participants were also given the opportunity to discuss issues they perceived relevant to the topic. Interviews lasted about one hour on average but ranged from 0.5 to 1.5 hours.

Procedure

Recruitment letters, including background to the study and contact details, were sent explaining the study to specific police departments that had been involved in the investigation of cyber-crime in one UK-based city. Participants confirmed their interest by contacting the first author to arrange a convenient time and location for the interviews. Prior to the interview, participants had opportunity to ask questions before informed consent was obtained and participants were fully debriefed following the interview with contact being maintained throughout data analysis. Ethical approval was obtained via the university's ethics committee and permission was sought from the police prior to recruitment.

Data Analysis

The data were digitally recorded, transcribed verbatim and analyzed using thematic analysis (TA) as described by Miles and Huberman (1994) as this method is well suited to exploring novel topics. According to Kelle (2006), TA *"can be used to gain access to local knowledge of the field in order to develop theoretical concepts and explanations that cover phenomena relevant for the research domain"* (p. 309). This includes situations such as the present study where there are small numbers of participants. The analytical process focused on a theoretical approach that used a latent way of analyzing the items. Braun and Clarke (2006) describe the theoretical approach *"to be driven by the researcher's theoretical or analytic interest in the area, and is thus more explicitly analyst-driven"* (p. 84). When dealing with a latent approach, the researcher looks deeper into the meanings and examines the undertones of the data. There were six steps used in the TA in the present study. These were: (i) familiarization with the data, (ii) generalizing initial codes, (iii) searching for themes, (iv) reviewing themes, (v) defining and naming themes, and (vi) producing the report.

Each interview was read and re-read to gain clarity, understanding, and to become close to the data (Braun & Clarke, 2006; Ryan & Bernard, 2003; Attride-Stirling, 2001). Each line of text was examined to identify key phrases of text and the researcher's thoughts were recorded in the margins. Codes were assigned to the key phrases to examine convergence and divergence between participants' narratives and identify key themes. An iterative process was followed to identify three emerging high-level themes and their associated sub-themes. Care was taken to ensure themes accurately reflected participants' narrative and a consistent approach was followed throughout the analysis.

RESULTS

Three main themes were identified comprising *online accessibility, threat,* and *the unhelpful victim and* are addressed in turn.

Theme 1: Online accessibility

Online accessibility was perceived as being advantageous to victims and perpetrators of cyber-harassment. For perpetrators, the internet provides access to victims' information about their victims. For victims, online behavior is recorded which aids police officers' investigations and evidence-gathering processes. Participants believed that high levels of online disclosure provide a wealth of information about victims and leaves them vulnerable to abuse. Social networking sites (SNSs) in particular were thought to provide a central location from which perpetrators could glean information relating to the victim and their social circle. This level of information cannot be obtained as easily in cases of offline harassment, makes cyberstalking-by-proxy easier, and increases vulnerability to offline harassment. For instance:

> **Extract 1:** *"[Perpetrators] get too much off [social networking] sites. You're just too easy to find, you're just leaving yourself wide open for anything"* (John).

Blame for cyber-harassment rested with victims who police officers perceived to have high levels of online self-disclosure:

Extract 2: *"[The victim] actually posted a journal, and it's really in-depth. He gets her mobile number off Facebook and again, she's made a mistake"* (Mike).

Allowing online users access to an individual's profile in SNSs, or accumulating 'friends', was associated with greater vulnerability to being cyber-harassed. The phrase 'every Tom, Dick and Harry' (Extract 3) is a colloquial phrase highlighting the uncontrolled and unknown properties of accumulating 'friends' who may not be known offline but are allowed access to personal information:

Extract 3: *"A lot of people are just getting friends and friends for no apparent reason. Allowing every Tom, Dick and Harry to visit their site, making yourself more of a target"* (Fred).

Online accessibility to victims also provides the opportunity for ex-partners to engage in harassing behaviors equivalent to domestic violence. Participants debated whether victims become upset by the content or quantity of messages sent in such cases. While Extract 4 below shows that it was the content of emails that was disturbing, Extract 5 emphasizes the number of text messages sent.

Extract 4: *"It was an ex-partner who was sending these email and some of the content was rather unpleasant"* (Jim).

Extract 5: *"When a couple have split up, they'll receive two hundred texts – Where are you? What are you doing?"* (John).

Arguably, the social presence of perpetrators is decreased in email communication due to the perception that there is more immediate access to victims using text messages. Therefore, large quantities of less threatening text messages may have a similar impact on victims as more explicitly threatening communications through less personal means.

Officers agreed that evidence is highly accessible in cases involving cyber-harassment and can be recovered despite deletion (although this may require considerable resources including time, cost, and manpower to investigate). Despite warnings by researchers that the evidence trail ends with a computer and not a person, participants were certain that perpetrators cannot abdicate responsibility for messages received by the victim:

> **Extract 6:** *"It doesn't matter if you press delete, doesn't mean it's gone. We can recall that information and prove where it's come from. They could say 'well I didn't send it' but you've allowed someone to use your computer to send it"* (Brendan).

In addition to victims maintaining records, participants explained that evidence could be retrieved from the website owners, as keeping copies of all Internet traffic is a legal requirement. This emphasizes the permanency of all online behavior which participants relied on when considering investigative action that could be taken:

> **Extract 7:** *"Once somebody types it in, it's there, it's logged, Facebook and Bebo, they all log it, they have to by law. They'll provide us with the information to do with IP addresses or email addresses and we're then able*

to request the information to establish who that particular person is. I mean, it's a long bit of work but it has to be done correctly for us to get that information" (Fred).

To summarize, participants perceived that online accessibility made their jobs as evidence-gatherers easier because records of all online activity is recorded. They also felt that victims increased their vulnerability to cyber-harassment with the amount of information they put online. This perception that victims should bear some responsibility was also evident in participants' perceptions that victims should maintain their own records of incidents of cyber-harassment.

Theme 2: Threat

Perpetrators' intentions to cause harm to victims was deemed crucial to investigations of cyber-harassment. Participants said that threats cannot be disregarded until intent is established. For instance:

Extract 8: *"You can't take a threat as not a threat until you…find out exactly what [the perpetrator's] intention is"* (Brendan).

Perpetrators issuing threats may be veiled or misdirected. One perpetrator threatened to kill themselves in front of the victim and the participant's use of language suggested the threat was perceived to be trivial yet the case resulted in murder. In Extract 9, the suggestion of 'something serious' happening may have been a veiled threat that is not recognized:

Extract 9: *"[The perpetrator threatened] "You don't know what I'm going to do…something serious is going to happen, I have a knife" he never really directly threatened to seriously harm her…more threatened to do silly things to himself and it'd be her fault…that's four or five days before the murder"* (Mike).

Participants regarded direct threats to harm as 'more serious' offences that are prosecuted under other Acts that carry harsher penalties than *PfHA*. This raises a fundamental question: if threatening violence against victims of harassment is dealt with using other criminal Acts, what is the purpose of Section 4 of the *PfHA*? For instance:

Extract 10: *"Somebody gets a text saying 'you know if you go to court, you would get', and there were threats. We classed it as witness intimidation"* (Pete).

Extract 11: *"I've had threats to kill but it's treated as a more serious offence"* (Fred).

Some participants discussed differences in how cyber-harassing behaviors may be perceived and the impact this could have on whether threats are taken seriously. Fred in Extract 12 emphasizes that the victim's description of their experiences will determine how seriously threats will be taken. By placing the emphasis on the victim's account, the participant relinquishes responsibility for the potential failure to investigate instances of cyber-harassment:

Extract 12: *"It could be 'I'm coming round right now to kick your head in'. You might read that in a completely different way than you would if someone said 'I'm having problems on the Internet, I'm getting quite a lot of messages, they're just abusive'"* (Fred).

Here, Extract 12 begins with a hypothetical threat that could be directed towards a victim on the Internet. The next sentence refers to 'you' perceiving that differently compared to someone saying they are receiving abusive messages via the Internet. The 'you' whom Fred was referring to appeared to be police officers who would interpret something the victim reports to them. Thus, the focus changes from threats a perpetrator might make to the way victims describe threats when reporting incidents to the police. Again, this demonstrates the way victims report cyber-crime to the police directly impacts on police officers' perceptions of the crime and whether the case is investigated. Mike retrospectively considered the police response if a victim they had worked with had reported cyber-harassment to the police.

Extract 13: *"I don't want to shoot ourselves in the foot really but…our young PCs would've gone…'[The perpetrator] lives in [another country, and] will never come'…If he lives in [a nearby city]'…we'd have said 'right, get rid of your Facebook…don't post on the net, become anonymous, can we try and get your flat moved?'…I'm not too sure how much our young cops would've done but at least we'd have had an opportunity"* (Mike).

Here, Mike believed that officers may have been unlikely to consider the threat posed by the perpetrator as viable as the perpetrator lived outside the UK. They felt that police officers would be more likely to offer the victim support and advice if the perpetrator lived in

the same country. Mike's tone reflected the difficulty perceived in considering the police response to a hypothetical scenario. Alternatively, Mike may have felt uncomfortable considering the possibility that officers may not act to protect a victim in similar circumstances as this contravenes police officers' ethos as protectors. The repetition of 'young' officers in Extract 13 highlights the lack of experience Mike perceived young police officers to have, and distanced Mike from such a scenario.

The accessibility of gathering evidence in cases involving cyber-harassment relies on accessing computers. Participants commented that seizing computers for forensic examination would be dependent on severity and some said they had not experienced such serious incidents:

> **Extract 14:** *"I've never actually had the extremes of seizing computers. No-one has taken it that far"* (John).

Similarly, Pete (Extract 15) said that seizing computers and cyber-forensic processes would be dependent on severity and whilst seizing computers would not be ruled out, harassment was not perceived to be serious, and resources would be retained for more serious crimes. Furthermore, the estimated time of forensic investigation of computers ranged from six weeks to eight months (Extract 16).

> **Extract 15:** *"Everything gets prioritized depending on what the crime is. Something serious like murder gets dealt with a lot quicker than something minor [like] harassment. I'm afraid it won't get put to the top of the list. One of the more serious jobs you have to submit an application form to the*

department that interrogates computers. It does take a good six weeks for it to get looked at" (Pete).

Extract 16: *"It's a good few months from submitting something for forensic analysis; you wouldn't expect to hear anything for six to eight months"* (Jim).

Whilst computers could be seized and examined, Fred (Extract 17) noted an important caveat that the seizure of computers cannot prevent cyber-harassment.

Extract 17: *"We will seize computers if we need to on as part of the investigation process. We just can't … prevent things happening"* Fred.

To summarize, participants considered that the perpetrator's intention to cause harm was an important element of their investigation into cyber-harassment. This finding is important as UK-based anti-harassment legislation does not require intent to be established. Legislation is victim-defined and the impact on the victim (causing distress or harm) determines whether a crime has taken place. This is subjected to the reasonable person's test. Furthermore, participants felt the credibility of threats in instances of cyber-harassment was questionable, especially when there is geographical distance between perpetrator and victim. When threats were perceived as credible, participants said they would use other legislative tools considered as more appropriate.

Theme 3: The Unhelpful Victim

'*The unhelpful victim*' was the final theme emerging and comprised of issues relating to the victim's behavior that participants considered unhelpful, frustrating, and undermining of their role when dealing with perpetrators. For some, victims were perceived as unwilling to follow through with complaints against the perpetrator. John (Extract 18) explained that victims want their complaint logged but refuse to allow officers to investigate incidents.

> **Extract 18:** *"The majority of the time [victims] will be unwilling to actually go forth [with] their complaint. They'll say "I just want to make you aware of this but I don't want to do anything about it". It is quite a hindrance, it is worrying"* (John).

The use of negative language in Extract 18 emphasizes the obstacles victims can introduce to cases. The tone illustrates frustration that implies that victims can waste officers' time. Brendan (Extract 19) stated victims are unlikely to allow officers to pursue investigations of between individuals who have had a romantic relationship.

> **Extract 19:** *"You go to arrest [the perpetrator]and the partner suddenly pleading with the police officer to leave them alone because they love them"* (Brendan).

These explanations align with descriptions of domestic violence and indicate that victims who have had a romantic relationship with the perpetrator will be less likely to pursue criminal action. Many participants said that victims are unwilling to change their online behavior that participants viewed as an important step in combating cyber-harassment.

Extract 20 echoes the frustration from Extract 19 as is evidenced in the repetition of victims described as 'unwilling to help themselves'. The frustration and disbelief expressed was with victims who are unwilling to change their behavior to protect themselves.

> **Extract 20:** *"The majority of the people are unwilling to leave social networking sites. They're unwilling to help themselves. They are unwilling to block that person or change their phone number, or contact their service provider. They just are unwilling to do it"* (John).

Fred (Extract 21) expressed frustration based on anticipated problems victims may face if their case proceeds to court.

> **Extract 21:** *"I find it really frustrating because I know that will be at the heart of a defense; the defense will be saying 'you're not being entirely truthful: If you're saying you're so scared, why did you not take yourself off Facebook? I put it to you that you're not that scared at all, you're actually enjoying it and you're doing this to get at my client!'"* (Fred).

Here, Fred imagined that the perpetrator's defense would focus on the victim not changing their behavior and using it as evidence that the victim was not distressed (a key requisite of the *PfHA*). By failing to change online behavior, the victim may undermine investigations carried out to bring a case to court. The majority of participants argued that the ability to prevent individuals from contacting a victim is a powerful tool that can prevent unwanted online contact. However, Mike (Extract 22) proposed that 'blocking' may be a catalyst for cyber-harassment escalating by moving offline and increasing threats posed.

> **Extract 22:** *"They use the phrase 'blocking' him, but they don't block him she knew 'if I block him that's like lighting the blue touch paper'. It's a complete diss. The first time that she blocks him he actively uses other people. Eventually, because they've blocked him, he uses the phone"* (Mike).

Here, the victim was reluctant to block the perpetrator because it would invoke anger: 'like lighting the blue touch paper'. Mike equated blocking someone online to offline ostracism, and this action fueled the perpetrator's anger towards the victim. Furthermore, the perpetrator found methods (other Internet users) to forward messages to the victim. Finally, 'blocking' acted as a catalyst for the escalation of harassing behaviors. Participants noted that withholding information caused difficulties for investigations of cyber-harassment. Officers emphasized the need to collate all available information about incidents for the CPS, and failure to have accurate information can limit officers' ability to do their jobs. For instance:

> **Extract 23:** *"We feed off intelligence: the less information we get, the less we can do about it"* (Sarah).

In particular, participants noted that victims may withhold information about their retaliation which is likely due to concern that police officers would form a negative opinion and may not pursue their case. Fred (Extract 24) explained that retaliation against the perpetrator is evidence of distress, but if officers discover information has been withheld, the victim be labeled a liar resulting in distrust.

Extract 24: *"If you've sent a message back that's abusive, I've got no problems with that. [It] shows how it's been for you. But you're portraying that you're actually a liar by not telling us everything"* (Fred).

To summarize, participants commented that victims of cyber-harassment can be unhelpful if and when they are investigating instances of cyber-harassment. Victims were perceived to be barriers to the evidence-gathering process and taking cases forward, particularly in cases involving domestic violence. Participants felt that victims were not helping themselves by changing their behaviors to prevent instances of cyber-harassment. However, one participant noted that such strategies (e.g., blocking) may actually escalate harassment.

DISCUSSION

This is the first UK-based study to explore police officers' perceptions of cyber-harassment, victims, and their role in dealing with cases. Three themes emerged – *online accessibility, threat,* and *the unhelpful victim*. *Online accessibility* revealed police officers' views about the vulnerability of Internet users in becoming victims of cyber-harassment and the ease of gathering evidence. *Threat* illustrated police officers' role as safety promoters and participants considered intent, harm, severity, and seizure of computers as indicative of the threat posed by perpetrators. *The unhelpful victim* highlighted frustrations of police officers towards victims who are perceived as unwilling in assisting them with their investigations.

Perceptions of cyber-harassment and victims

Police officers perceived the increasing accessibility of the Internet and online self-disclosure were contributory factors to cyber-harassing vulnerability. They emphasized that rapid technological advances mean that perpetrators can access victims 'at the touch of a button'. Researchers have previously speculated that the prevalence of cyber-harassment would increase as people incorporated online technology in their lives (e.g., Cupach & Spitzberg, 2004; Salter & Bryden, 2009), and police officers' perceptions reflect this. Younger individuals were perceived more vulnerable to cyber-harassment compared to older individuals. This suggests an age-related digital divide for cyber-harassment victimization which is likely because Internet users tend to be younger (Dutton & Helpser, 2007; Granello & Wheaton, 2004). However, Gilleard and Higgs (2008) argue the age-related digital divide is generational rather than reflective of stage of life and will dissipate in the future.

Police officers were concerned about online self-disclosure and the 'friending' culture (i.e., accumulating 'friends' who may not be known to individuals). This was perceived to be most prevalent among social networking sites (SNSs). Social identification mode of deindividuation (SIDE) theory explains that computer-mediated communication (CMC) increases the saliency of either social or personal identity (Spears, Lea & Postmes, 2007). When social identity is salient, individuals are expected to adhere to group norms and adhere to their own standards when personal identity is salient. Within CMC, anonymity plays an important role in increasing the saliency of either social or personal identity. When online, anonymity can be either visual (anonymity of others to self) or lack of identifiability (anonymity of self to others; Joinson, 2001). Lack of identifiability emphasizes social isolation as individuals perceive themselves as separate from the group and visual anonymity increases attraction within the group and heightens self-awareness (Lea, Spears & de Groot,

2001). Consequently, the salience of physical and affective states is increased, contributing to self-disclosure.

Arguably, SNSs increase the salience of social identity and SIDE theory predicts adherence to group norms. Within SNSs, self-disclosure and 'friending' is the cultural norm with the refusal of 'friend requests' (even from strangers) is inappropriate (boyd, 2006; Tong, Van Der Heide, Langwell, & Walther, 2008). Self-disclosing in SNSs, promotes group cohesion, contributes to a sense of community, and increases attraction within (and to) the group. Potentially detrimental online behaviors, (e.g., 'friending' and self-disclosure) are self-promoting and meaning individuals may willingly but unknowingly provide perpetrators access to a wealth of information. People may not adhere to the safety standards they would normally apply in their offline lives which concerned the police officers in the present study.

Participants explained cyber-harassed victims were ultimately unwilling to change their online behavior and this was viewed an important step in minimizing further harassment. Behavioral changes recommended included withdrawal from SNSs, becoming anonymous online, and/or blocking the perpetrator. Bocij (2004) argued that avoiding online spaces contravenes individuals' human rights. Furthermore, this violates social norms and could further victimize individuals. However, self-protection strategies are used in offline everyday life, and individuals may be in a position to take responsibility to protect themselves from cyber-harassment (Basu & Jones, 2007; Salter & Bryden, 2009).

Participants expressed frustration at victims' unwillingness to protect themselves whilst online as this could be used as evidence against them if their case was brought to court. The perpetrator's defense could argue that the victim was not impacted to the extent proposed. This could be evidenced by their reluctance to change their online behavior in an attempt to avoid the perpetrator. Victims can also minimize their own behavior towards the perpetrator which can reduce their credibility if uncovered. Police officers perceived that

being unwilling to change online behavior and withholding contextual information undermines investigations.

Failure to disclose information to police officers contrasts with victims' online self-disclosure. According to media richness theory, individuals prefer different forms of media to relay messages dependent upon reducing equivocality and uncertainty (Daft & Lengel, 1986). In face-to-face (FtF) communication, individuals have immediate feedback through body language, tone of voice, message content, and a variety of language – but this is reduced in CMC (Rice, 1992). As lying is equivocal (Whitty & Joinson, 2009), individuals are more likely to lie in rich media (such as FtF). This creates tension between police officers' need to collate all relevant information and victims' desire to engage in impression management strategies (including lying about their own behavior) to ensure their case is taken seriously. It may be beneficial for victims to know that this type of behavior illustrates the impact of cyber-harassment rather than damaging their case.

Police officers in this study were divided in the perceived usefulness of 'blocking' perpetrators. The majority suggested blocking as a primary strategy to deter perpetrators and this strategy is reiterated in publications available to the general public (e.g., O'Connell, Price & Barrow, 2004). However, Mike (Extract 22) illustrated that blocking can be ineffective and may escalate pursuit behavior by the perpetrator. Although speculative, there may be a threshold during a cyber-harassing campaign before which blocking is effective in deterring the cyber-harasser. Once the threshold is passed, the perpetrator's motives may be strengthened and blocking may not deter them or may result in escalation.

Participants were concerned at victims' unwillingness to follow through with allegations against perpetrators, particularly in instances involving domestic abuse. In such instances, victims wanted officers to record complaints but not take any action. The link between cyber-harassment and domestic abuse supports research suggesting that domestic

violence plays a role in offline harassment. Coleman (1997) argued that leaving an abusive partner is ineffective and dangerous as it may lead to harassment. The association between domestic abuse and cyber-harassment may be evidence that perpetrators of domestic violence are embracing new technologies to continue partner abuse. As Coleman's research highlighted, victims of domestic abuse may be aware that pursuit of legal action may prove dangerous and ineffective. Thus, victims may not wish to pursue complaints because they fear further reprisals which may explain the reluctance of victims following through with complaints made as described by police officers in the present study.

Arguably, it could be suggested that participants' cumulative views of cyber-harassed victims indicated victim-blame. Participants considered victims to be responsible for their victimization as a result of their high-levels of online disclosure and reluctance to utilizing self-protection strategies. Victims were also seen to be responsible for maintaining records of incidents of cyber-harassment with no apparent consideration that maintaining records may impact on victims' mental wellbeing. Ultimately, victims were perceived as 'unhelpful', acting as barriers to their roles as evidence-gatherers.

Combating cyber-harassment

Participants believed that dealing with cyber-harassment formed part of their role as a police officer and lends support to research conducted by Kamphuis, Emmelkamp and deVries (2004). More specifically, police officers perceived their role solely as evidence-gatherers and participants said that evidence is accessible by contacting Internet service providers (ISPs), website owners, and/or by seizing and analyzing computers. As there is a digital trace of all online behavior, participants believed it is possible to trace perpetrators offline despite attempts to remain anonymous. This finding contradicts Bocij (2004) and Griffiths, Rogers and Sparrow's (1998) assumption, but this is because technology and cyber-

forensic techniques have evolved since the authors' time of writing. The perceived accessibility of evidence is encouraging and may encourage victims to report cyber-harassment to the police.

Contrary to recommendations for investigating cyber-harassment (Brown, 2000), police officers in the present study suggested that victims do not need to keep messages containing harassment because such evidence is easily accessible. However, it is unlikely that instances of cyber-harassment would be investigated without evidence of the perpetrator's behavior. Whilst police officers reported positive steps they can take to investigate cases involving cyber-harassment, the severity of the cases determined what action they could take. For the most serious cases (defined by participants as threats to life), police officers can issue harassment warnings, seize computers, and contact website owners and/or ISPs to retrieve evidence. Therefore, the resources (time and financial) required gathering evidence from formal sources (e.g., ISPs) mean that obtaining this type of evidence is unlikely if the threat towards the victim is perceived to be minimal. Furthermore, UK courts limit the coverage of anti-harassment legislation and there are precedents to ensure that only the most severe cases of harassment proceed to court (Salter & Bryden, 2009). As officers are responsible for enforcing the law, police officers' perceptions of severity in the present study reflect the court precedents.

In the present study, the severity of potential harm to the victim was associated with the credibility of threats made. The credibility of CMC-mediated threats has been questioned, especially in cases whereby the perpetrator lives outside the UK (Burgess & Baker, 2002). The present study found that if perpetrators live outside the UK, it is unlikely that police officers will take the victim's complaint seriously. Despite this, Mike (Extract 13) demonstrated that perpetrators can travel from other countries specifically to carry out threats made. Sheridan and Grant (2007) found that cyberstalked victims are threatened to the same

degree as victims of offline harassment. Thus, the view that such threats are minimized reinforces concerns made by other researchers (e.g., Bocij & McFarlane, 2003), and suggests that victims may not be given the full protection of the law.

Limitations

The present study, while rich in data, has a number of limitations. The findings cannot be generalized due to the small sample size and because participants were recruited using snowball sampling. Consequently, all participants were self-selecting volunteers and worked in a single UK-based police force. This may have introduced bias as only those officers who believed they were knowledgeable in dealing with cyber-crime may have volunteered to participate. Furthermore, there are many different police forces within the UK that may have different procedures in dealing with crime. The present study may be useful to inform a quantitative survey that would be useful to confirm and elaborate upon the current findings.

Police officers in the present study often focused on severity and threats posed to victims of cyber-harassment. Whilst examples of serious threats were given (e.g., threat to life), the notion of threat and severity was ambiguous. Furthermore, the study did not investigate police officers' perceptions of cyber-harassment whereby perpetrators did not or implicitly threaten victims. Consequently, the findings may be most beneficial for victims of severe cyber-harassment and those who have been explicitly threatened by perpetrators.

As semi-structured interviews were conducted, the police officers were identifiable by the researcher and their colleagues if recruited via snowball sampling and this may have increased the salience of participants' profession. Consequently, participating police officers may have been reluctant to portray negative perceptions about their ability in dealing with cyber-harassment and keen to portray a positive image of the police force. This may have impacted on the ecological validity of the research.

Future Research

The findings of the present study suggest possible avenues for future research. For instance, a vignette study manipulating the type and credibility of threats made to victims would be beneficial to explore perceived severity of cyber-harassing behaviors. Items relating to the vignettes could establish whether police intervention is perceived as necessary and the types of actions that should be taken. This type of study could recruit Internet users and police officers to establish differences in perceptions and identify differing expectations. Further research would benefit from recruiting social networking users and examining attachment to social networking profiles to gain insight into how users can be better protected in these online spaces. To triangulate the findings of the present study, it would also be useful to explore the experience of cyber-harassed victims have contacted the police. Such research could focus on remedies offered by police officers dealing with their case and the perceived usefulness of remedies offered.

Implications and conclusions

The present study has several implications for social policy and cyber-harassed victims. Police intervention depends on the severity of the perpetrator's behavior and threats made to victims. However, stalking often involves behaviors that appear benign unless viewed in the context of a campaign against the victim (Hills & Taplin, 1998). Threats made may not be explicit and thus may not be perceived as credible by police officers. In conjunction with the precedent set in UK courts ensuring only the most serious of harassment cases proceed to prosecution, police officers may not be able to offer support to the majority of cyber-harassed victims.

If police officers cannot protect the majority of victims, Internet users need to protect themselves more while online to reduce their vulnerability. This need for self-protection is more pronounced with increased use of social networking sites and 'friending' cultures. 'Friending' strangers or near-strangers can be positive as it offers a unique way for individuals to increase their social circles and may reduce social isolation among vulnerable individuals. However, those who 'friend' strangers need to be aware of the risks associated with allowing strangers access to information about their lives. SNS service providers should take greater responsibility for users' knowledge of how to use their site and privacy settings. For example, *Facebook* is a popular SNS and privacy settings allows users to customize which 'friends' can access information on their profile. *Facebook* could regularly send all users an email that highlights this feature and explains how and why this can be used.

Furthermore, SNS service providers could use greater measures of control that can be helpful to investigations of cyber-crime. Providers could routinely request details from users to confirm their identity before allowing access to the site. This would make it easier for officers to trace perpetrators if they use SNSs to commit crime. Service providers could also make it easier for officers to contact them by issuing a contact email address or telephone number that is only available to police officers.

The *PfHA* appears sufficiently broad to incorporate all forms of harassment and does not require burden of proof of the perpetrator's intent. However, application of the Act is more complicated and precedents restrict the usefulness of the Act in prosecuting cyber-harassment. Whilst Section 4 allows for more serious forms of harassment to be prosecuted, police officers use other laws to deal with more serious threats. This highlights the need for more detailed guidelines to be issued regarding the application of the Act to real examples of both offline and online harassment. This would provide police officers and victims clear ideas

regarding instances when the Act provides coverage. Despite the new powers afforded by the *PoFA* (2012), there are still no legislative powers when the perpetrator lives outside the UK.

Finally, police procedures in dealing with cyber-harassment should be transparent to the general public. Police officers in the present study perceived victims as unhelpful when they request digital hardware to gather evidence or ask them to change their online behavior. Previous research suggests that victims are dissatisfied with action taken by police officers (e.g., Finn, 2004) and this may be confounded with the time taken to investigate instances of cyber-harassment. Victims should be clearly informed of what will be required from them, why, and investigative timescales upon first contact. This may increase victims' satisfaction with how their case is dealt with, encourage victims' co-operation, and ultimately encourage victims to report cyber-harassment to the police.

REFERENCES

Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research. *Qualitative Research, 1*, 385-405.

Basu, S., & Jones, R. P. (2007). Regulating cyberstalking. In F. Schmalleger & M. Pittaro. (Eds.). *Crimes of the Internet*. UK: Prentice Hall.

Blaauw, E., Winkel, F. W., Arensman, E., Sheridan, L., & Freeve, A. (2002). The toll of stalking: the relationship between features of stalking and psychopathology of victims. *Journal of Interpersonal Violence, 17*, 50–63.

Bocij, P. & McFarlane, L. (2003). Cyberstalking: a matter for community safety – but the numbers do not add up. *Community Safety Journal, 2*, 26-34.

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*. Westport, Connecticut: Praeger.

Bocij, P., Griffiths, M., & McFarlane, L. (2002). Cyberstalking: A new challenge for criminal law. *The Criminal Lawyer, 122*, 3-5.

boyd, d. (2006). Friends, friendsters, and top 8: writing community into being on social network sites. *First Monday 11, Article 10*. Retrieved March, 26, 2010, from: http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.phplfm/article/view/1418/1336.

Braun, V & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*, 77-101.

Broll, R. & Huey, L. (2014). "Just being mean to somebody isn't a police matter": police perspectives on policing cyberbullying. *Journal of School Violence, 14*(2), 155-176.

Brown, H. (2000). *Stalking and Other Forms of Harassment: An Investigator's Guide*. Metropolitan Police Service. London, UK: Home Office.

Budd, T., & Mattinson, J. (2000). *The extent and nature of stalking: Findings from the 1998 British Crime Survey*. (Home Office Research, Research Study No. 210). London: Research Development and Statistics Directorate.

Burgess, A. W., & Baker, T. (2002). *Cyberstalking. In J. Boon, & L. Sheridan (Eds.), Stalking and Psychosexual Obsession: Psychological Perspectives for Prevention, Policing and Treatment*. West Sussex: Wiley.

Coleman, F. L. (1997). Stalking behaviour and the cycle of domestic violence. *Journal of Interpersonal Violence, 12*, 420-432.

Cupach, W. R., & Spitzberg, B. H. (2004). *The Dark Side of Relationship Pursuit: From Attraction to Obsession and Stalking*. Mahway, New Jersey: Lawrence Erlbaum Associates.

Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness, and structural design. *Management Science, 32*, 554-571.

Draucker, C. B. (1999). "Living in hell": The experience of being stalked. *Issues in Mental Health Nursing, 20*, 473-484.

Dreβing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (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.

Dutton, W., & Helsper, E. J. (2007). *The Internet in Britain: 2007*. Oxford Internet Institute, University of Oxford. Oxford: UK.

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

Fremouw, W. J., Westrup, D., Pennypacker, J. (1997). Stalking on campus: The prevalence and strategies for coping with stalking. *Journal of Forensic Science, 42*, 666-69.

Gilleard, C., & Higgs, P. (2008). Internet use and the digital divide in the English longitudinal study of ageing. *European Journal of Ageing, 5*, 233-239.

Granello, D. H., & Wheaton, J. E. (2004). Online data collection: Strategies for research. *Journal of Counseling & Development, 82*, 387–393.

Griffiths, M. (1999). Cyberstalking: A cause for police concern? *Justice of the Peace, 163*, 687-689.

Griffiths, M., Rogers, L., & Sparrow, P. (1998). Crime and IT: "Stalking the Net'. *Probation Journal, 45*, 138-141.

Hills, A. M., & Taplin, J. L. (1998). Anticipated responses to stalking: Effect of threat and target-stalker relationship. *Psychiatry, Psychology and Law, 5*, 139-146.

Home Office. (1997). *Protection from Harassment Act 1997*. London: HMSO.

Home Office (2012). Protection of Freedoms Act 2012. London: HMSO.

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology, 31*, 177-192.

Kamphuis, J. H., Emmelkamp, P. M. G., & de Vries, V. (2004). Informant personality descriptions of postintimate stalkers using the five factor profile. Journal of *Personality Assessment, 82*, 169-178.

Kaur, M., Kaur, N., & Khurana, S. (2016). A literature review on cyber forensic and its analysis tools. *International Journal of Advanced Research in Computer and Communication Engineering, 5*(1), 23-28.

Kelle, U. (2006). Combining qualitative and quantitative methods in research practice: purposes and advantages. *Qualitative Research in Psychology, 3*, 293-311.

Lea, M., Spears, R., & de Groot, D. (2001). Knowing me, knowing you: anonymity effects on social identity processes within groups. *Personality & Social Psychology Bulletin, 27*, 526-537.

Miles, M., & Huberman, M. (1994). *Qualitative Data Analysis: An expanded sourcebook*. London, UK: Sage.

Morris, S., Anderson, S., & Murray, L. (2002). *Stalking and Harassment in Scotland*. Research Findings No. 67/2002. Scotland, UK: Scottish Executive.

O'Connell, R., Price, J., & Barrow, C. (2004). *Cyberstalking, Abusive Cyber Sex and Online Grooming*. Centre for Cyberspace Research, Preston.

Roberts, A., R., & Dziegielewski, S. F. (1996). Assessment typology and intervention with survivors of stalking. *Aggression & Violent Behavior, 1*, 359-368.

Ryan, G.W., & Bernard, H.R. (2003). Techniques to identify themes. *Field Methods*, *15*, 85-109.

Salter, M., & Bryden, C. (2009). I can see you: harassment and stalking on the Internet. *Information & Communications Technology Law*, *18*, 99–122.

Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law, 13*, 627-640.

Short, E., Guppy, A., Hart, J.A., & Barnes, J. (2015). The impact of cyberstalking. *Studies in Media and Communication*, *3*(2), 23-37.

Sinclair, K.O., Bauman, S., Poteat, P., Koenig, B., & Russell, S.T. (2012). Cyber and bias-based harassment: associations with academic, substance use, and mental health problems. *Journal of Adolescent Health, 50*, 521-523.

Spears, R., Lea, M., & Postmes, T. (2007). Computer-mediated communication and social identity. In A. Joinson, K. McKenna, T. Postmes, & U-D. Reips (Eds.), *The Oxford Handbook of Internet Psychology* (pp. 253-269). Oxford, UK: Oxford University Press.

Tjaden, P., & Thoennes, N. (1998). *Stalking in America: Findings from the National Violence Against Women Survey*. No. 93-IJ-CX-0012. Washington, DC: U.S. Department of Justice.

Tong, S, Van Der Heide, B., Langwell, L., & Walther, J. (2008). Too much of a good thing? The relationship between number of friends and interpersonal impressions on Facebook. *Journal of Computer-Mediated Communication, 13*, 531–549.

Wall, D. S. (1998). Catching cybercriminals: Policing the Internet. *International Review of Law, Computers & Technology, 12*, 201-218.

Wall, D. S., & Williams, M. (2007). Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology and Criminal Justice, 7*, 391–415.

Whitty, M. T., & Joinson, A. N. (2009). *Truth, Lies and Trust on the Internet*. East Sussex, UK: Routledge.

Yeboah-Boateng, E. O., & Akwa-Bonsu, E. A. (2016). Digital forensic investigations: issues of intangibility, complications and inconsistencies in cyber-crimes. *Journal of Cyber Security, 4*, 87-104.