Technology, Cyberstalking and Domestic Homicide: Informing Prevention and Response Strategies

Chris Todd[1], Joanne Bryce[2] and Virginia N. L. Franqueira[3]

Abstract

An emerging concern in relation to the importance of technology and social media in everyday life relates to their ability to facilitate online and offline stalking, domestic violence and escalation to homicide. However, there has been little empirical research, or policing and policy attention to this domain. This study examined the extent to which there was evidence of the role of technology and cyberstalking in domestic homicide cases based on analysis of 41 Domestic Homicide Review (DHR) documents, made available by the Home Office (UK). Three interviews were also conducted with victims or family members of domestic homicide in the UK. It aimed to develop a deeper understanding of the role of technology in facilitating these forms of victimisation to inform further development of investigative practice, risk assessment and safeguarding procedures. Key themes identified by the thematic analysis undertaken related to behavioural and psychological indicators of cyberstalking, evidence of the role of technology in escalation to homicide, and the digital capabilities of law enforcement. Overall, the results indicated that: (1) there was evidence of technology and social media playing a facilitating role in these behaviours, (2) the digital footprints of victims and perpetrators were often overlooked in police investigations and the DHR process, and (3) determining the involvement of technology in such cases is important for risk assessment and earlier intervention to prevent escalation of behaviour to domestic homicide. It also indicates the importance of further developing evidence-based approaches to preventing and responding for victims, the police and other practitioners.

Keywords: Domestic Violence, Cyberstalking, Domestic Homicide Review (DHR), Technology, Social Media.

[1] *West Midlands Police, West Midlands Police Headquarters, Birmingham, UK*

[2] *School of Psychology, University of Central Lancashire, Preston, Lancashire, UK*
jbryce@uclan.ac.uk (corresponding author)
ORCID: 0000-0001-9144-2899

[3] *School of Computing, University of Kent, Canterbury, Kent, UK*
v.franqueira@kent.ac.uk (corresponding author)
ORCID: 0000-0003-1332-9115

Introduction

The internet and social media are increasingly involved in the initiation and maintenance of romantic relationships (Carpenter & Spottswood, 2013; Dimond et al., 2011). Although they can facilitate closeness and intimacy between romantic partners, they can lead to negative behaviours that are damaging to the individuals involved and the relationship (e.g., monitoring of social media accounts, online interactions) (Blais et al., 2008; Marcum et al., 2016; Ybarra et al., 2017). There are also concerns about the potential for these technologies to facilitate online and offline stalking, domestic violence and escalation to homicide (Finn & Atkinson, 2009; Woodlock et al., 2019). Despite this, there has been relatively little empirical research, or policing and policy attention to the role of social media and new technology in these categories of offending (Woodlock et al., 2019; Ybarra et al., 2017). As a result, there is limited understanding of their use by offenders to conduct surveillance and control their partners during, or after the end of a relationship (Henry & Powell, 2016; Woodlock, 2017). It is important to develop more detailed knowledge about this issue in order to identify common behavioural patterns and potential risk factors. This can inform the development of evidence-based approaches to preventing and responding to stalking, domestic violence and homicide for the police and other practitioners. This paper contributes to this emerging area of research by examining the intersection of technology and social media with these forms of offending and victimisation.

The Home Office (2013a) defines domestic abuse as:

> "Any incident or pattern of incidents of controlling or threatening behaviour, violence or abuse between those aged 16 or over who are or have been intimate partners or family members regardless of gender or sexuality. This can encompass but is not limited to the following types of abuse: Psychological, physical, sexual, financial, emotional." (UK Home Office, 2013a)

Police crime figures indicated that there were 559,549 domestic abuse incidents recorded in England and Wales in the year ending March 2018 (Home Office, 2018). Given that it is known that only a small proportion of domestic abuse incidents are reported to the police (e.g., Walby et al., 2015), these

figures are not directly comparable with victimisation estimates from the Crime Survey for England Wales (CSEW), which include unreported incidents and focuses on the number of victims rather than the number of recorded crimes (Home Office, 2018). The CSEW for the year ending March 2018 estimated that there had been two million domestic abuse incidents during this period. Females were more likely to report this experience compared to males (7.9% and 4.2% respectively), equivalent to an estimated 1.3 million female and 695,000 male victims (Home Office, 2018). The majority of these incidents related to intimate partner violence, with females also being more likely to report this experience than males (6.3% and 2.8% respectively) (Home Office, 2018). These figures suggest that intimate partner violence is under-reported and affects more females than males, and is a gendered crime (Walby et al., 2015).

A key reason for the lack of victim reporting relates to the dynamics which characterise these relationships, particularly the use of coercive control, which is often unseen by those outside the relationship (Hardesty et al., 2015; Stark, 2012). It can manifest itself in a variety of ways, including withdrawal of financial resources, isolation from family and friends, continual emotional and psychological abuse, or sexual violence; none of which need necessarily be evident to anyone other than the victims themselves (Day & Bowen, 2015; Hardesty et al., 2015). The use of coercive control strategies has been found to be associated with persistent and serious physical violence in relationships, including the risk of being a victim of domestic homicide (Day & Bowen, 2015; Richards, 2003).

Domestic homicide refers to victims killed by a partner/ex-partner, relative or someone else living with them at the time (Home Office, 2018). This type of violence results from a process of victimisation and does not remain hidden as a result of the extreme nature of its outcome. There is a clear gender bias in victimisation, with the majority of the victims in the 400 domestic homicides recorded by the police in England and Wales between April 2014 and March 2017 being female and the perpetrator being a male partner or ex-partner (Home Office, 2018). This does not mean that females are never

perpetrators, and highlights the need to ensure that adequate support is also provided for male victims of domestic violence (Monckton-Smith et al., 2014).

A key issue relating to domestic violence and homicide is the importance of determining predictors that enable the identification and safeguarding of those most at risk of victimisation and escalation of violence. The DASH risk assessment (SafeLives, 2014) is used by UK agencies to achieve this aim and determine appropriate agency responses. It contains items relating to offender behaviour and victimisation experiences identified as significant predictors of serious violence and homicide. This includes attempts by the victim to separate from their abuser and evidence of coercive control (UK Home Office, 2013b). It also contains a question related to the experience of stalking or harassment (specified as *"constant/obsessive phone calls, texts or emails")* which has been identified as an indicator of high risk of escalation and harm (SafeLives, 2014). The inclusion of this question reflects the use of stalking by perpetrators to exert control over their victim and monitor their behaviour during the relationship, as well as when they endeavour to separate or after the end of a relationship (Roberts, 2005; Stark, 2012). This is consistent with research suggesting that violence occurs in the majority of stalking cases involving ex-partners, and has been identified as a risk factor for the escalation of violence in domestic abuse and homicide (Finn & Atkinson, 2009; Sheridan & Roberts, 2011).

Stalking and Cyberstalking

The Protection from Harassment Act (1997) identifies a number of examples of stalking behaviours, including: following a person in their day to day activities or lives; contacting, or attempting to contact, a person by any means (e.g., phone, email, text); monitoring the use by a person of the internet, email or any other form of electronic communication; and watching or spying on a person. The inclusion of behaviours involving technology, social media and surveillance applications reflects the increasing recognition that these are facilitators of coercive control and stalking, as well as the escalation of violence and homicide (Elphinston & Noller, 2011; Finn & Atkinson, 2009; Tokunaga & Gustafson,

2014). This may be particularly relevant where the victim communicates the intention to end the relationship or leave the perpetrator, or they seek to re-establish the relationship after separation (Cavazza & McEwan, 2014; Reckdenwald & Parker, 2010). This is evidenced by research suggesting that the National Stalking Helpline responded to a total of 4,659 contacts in the year ending March 2018, and 727 of those confirmed their stalker was an ex-partner or family member (ONS, 2018). 80% of this sample were female, and 78% were being stalked by a male ex-partner (95%), suggesting a similarly pattern of gendered behaviour to domestic violence This highlights the need to further examine the intersection between these behaviours and experiences, in relation to the escalation of domestic violence and homicide in order to develop effective prevention and response strategies (Finn & Atkinson, 2009; Henry & Powell, 2016; Woodlock, 2017).

Victim impacts and responses

Although there is potential for domestic homicide to result from stalking and cyberstalking, research also suggests that their experience can have significant negative impacts on the psychological and physical health of victims (e.g., fear, anxiety, depression, trauma and PTSD) (e.g., Hakkanen-Nyholm, 2010). Victimisation can also lead to adjustments to offline life and activities as people change jobs or change their socialising activities as a result of the fear of being followed or physically assaulted (Maple et al., 2011).

Victim strategies for coping and responding to stalking and cyberstalking include confronting or trying to reason with the perpetrator, denying the problem, seeking escape through substance and alcohol abuse, and seeking third party support (e.g., friends and family, reporting to the police) (Bjorklund et al., 2010; Logan & Walker, 2017; Ybarra et al., 2017). Research suggests that reporting victimisation experiences to the police appears to be much less frequent, with one study finding that only 5% of cyberstalking victims took such action (Duggan et al., 2014). This is consistent with recent research which found that only 21% of victims of UK domestic violence reported their experiences (Home

Office, 2016). Of those who did not make an official report, 25% did not think they could be helped and 37% felt their experiences were a private matter. Embarrassment or fear that experiences will be minimised are also a barrier to victim reporting (Henry & Powell, 2016). This is consistent with the recognition that law enforcement responses to domestic violence are variable (UK HMIC, 2014), and such perceptions are a significant barrier which may increase risk of harm to victims.

This is recognised by national policing and features heavily in the current national strategy (College of Policing, 2015; UK HMIC, 2019). It is supported by partner agencies and the third sector through the Violence Against Women and Girls Strategy (UK HM Government, 2016). Third sector agencies have worked effectively to develop specific guidance for victims of digital stalking as exemplified by Perry's (2012) collaboration between the Network for Surviving Stalking and Women's Aid. However, it is clear that further empirical, policy and political attention to the issue is required in order to develop a deeper understanding of the role of technology and cyberstalking in domestic violence and homicide (Dimond et al., 2011; Woodlock et al., 2019). This can then inform appropriate investigative strategies and resource deployment as per the National Intelligence and National Decision Models (Centrex, 2008; College of Policing, 2016), and the development of strategies to ensure that practitioners are aware of the role of technology and social media in facilitating victimisation, as well as providing effective education for victims about prevention and help-seeking strategies (Henry & Powell, 2016; Woodlock et al., 2019).

Aims of the Study

As a result, this study aimed to address these issues by examining:

(1) The extent to which stalking and cyberstalking were involved in domestic homicide cases on the basis of the analysis of Domestic Homicide Review (DHR) documents. This included cases

where these behaviours were specifically identified as playing a key role in escalation of domestic homicide, and where evidence existed that this may have been the case.

(2) The perspectives of victims or family members of victims of domestic homicide which involved cyberstalking through conducting a small number of semi-structured interviews examining the role of technology and limitations in the investigative and safeguarding procedures implemented by stakeholders.

Method

Design

This study used a qualitative methodology to address the research aims. It consisted of two inter-related phases. The first utilised a thematic approach to analyse the content of domestic homicide review documents (DHRs) (Braun & Clarke, 2006). The second phase involved the conduct of a small number of semi-structured interviews with individuals who were victims or family members of victims of domestic homicide.

Sample/procedure

DHR review

Since 2011, the Home Office has directed that every death in the UK appearing to result from domestic abuse where the victim was aged 16 years or over should be subject of a domestic homicide review (DHR) (UK Home Office, 2011). It is the local authority's responsibility to establish DHR panels and publish findings. Therefore, where criminal proceedings and parallel enquiries are finalised, and no matters remain *sub judice,* a detailed multi-agency report is potentially available for most domestic homicides in England and Wales. The Home Office Domestic Homicide Review Team was approached and provided a sample of 53 DHRs published between 2011 and 2014. These were filtered to identify a sample of 41 which specifically related to intimate partner abuse, and were therefore

relevant to the aims of the study. Where gaps in biographical data were evident, open source research was conducted to identify the relevant information (Crowe & Davidson, 2009). The ease with which this was completed highlighted the need to introduce additional layers of anonymisation before data analysis and write up.

Interviews

Three individuals were approached and invited to take part in an interview. They were selected on the basis that all were actively engaged in promoting awareness of intimate partner abuse and known to one of the researchers. One participant was the victim of attempted murder and stalking. The others were parents of domestic homicide victims. All three were experienced in presenting to law enforcement audiences in the course of their support work, and were therefore both accessible and pre-assessed as reliable sources. They had all been directly affected by domestic homicide and had valuable experiences to share as a result. The interviews were conducted by one of the authors face to face and by telephone. In each instance the interview was recorded and anonymised at the point of transcription before coding. The interviews lasted between 25 and 45 minutes. Each participant was given full ethical information about the research and provided informed consent prior to the start of the interview session.

Materials / interview schedule

The second method of data collection used semi-structured interviews to enable the participants to address the research aims, whilst providing them with the opportunity to provide an in-depth understanding of their experience (Bogdan & Biklan, 2007). The interview questions were constructed in a manner designed to elicit the personal experiences of the participant, regardless of the extent to which cyberstalking had been evident in the formal investigations undertaken, and to further probe issues raised where appropriate. For example, participants were asked *'To what extent did the perpetrator monitor the victim's online activity covertly*?'

Ethics

Ethical approval for both phases of the study were obtained by the institutional ethics committee. Each DHR was allocated a unique reference number to ensure the anonymity of the individuals involved in the cases addressed. All interview participants were engaged in public speaking about their experiences to increase awareness and provide victim support. They were not asked to discuss anything more detailed than they would otherwise do in the course of their public speaking in order to minimise the risk of causing distress. Briefing materials were provided to the participants before the interview session to ensure the ability to provide informed consent to participate.

Data Analysis

Document analysis was the primary focus of the study, and the analysis involved an iterative process combining elements of content and thematic analysis (Braun & Clarke, 2006). Analysis of these documents was advantageous given their accessibility, authenticity and the associated confidence the researcher can have in their content (Bowen, 2009), knowing that they have been prepared for public scrutiny and in order to hold contributing agencies to account (UK Home Office, 2011). In the initial stage of analysis, specific codes and themes were identified on the basis of the aims of the study. These included evidence of coercive control, emotional abuse and physical violence. It also included coding for use of specific device types and online platforms to facilitate online harassment and stalking (e.g., mobile phones, text messaging, social media). The next stage involved an iterative process of revising the documents and transcripts in order to achieve data familiarisation, and to further develop and refine the initial list of identified coding labels and identify emergent themes (Braun & Clarke, 2006). Each time a new code or theme was identified, every document and interview was reviewed to eliminate the opportunity of oversight in previous readings.

The interviews were recorded and transcribed. Anonymisation was undertaken at this stage to provide unique reference numbers for each and remove any potential identifiers in the data to maintain

anonymity and confidentiality. The process of data analysis, coding and theme identification followed the same steps as described above.

Results

Of the 53 DHRs received, 41 related to domestic homicide. These were coded to identify prevalence of cyberstalking and use of technology in addition to the three contextual interviews. Coding for other relevant factors (e.g., control, separation, physical surveillance) and emergent themes was also undertaken. The findings presented here relate to the 41 DHRs and three contextual interviews where the victims and perpetrators were intimate partners.

Demographic Characteristics

The ages of victims in the cases reviewed by the DHRs ranged from 20 to 80 years of age (mean = 43 years). Perpetrators were aged between 21 and 69 years (mean= 46 years). The perpetrators were male in 80.5% of the DHRs reviewed and all their victims were female. This is consistent with research suggesting that females are victims in 89% of all intimate partner homicides in the UK (ONS, 2014b) and the claim the gendered nature of the crime (Monkton-Smith et al., 2014). Of the remaining 19.5% cases, where females were the perpetrators against male victims, 62.5% of cases presented evidence that they had themselves been abused by their partner before the homicide. There was no evidence of any of the male perpetrators having been previously abused by their partners. This also suggests that many women are driven to kill as a means of escaping chronic abuse (Dermody-Leonard, 1997).

Identification of Perpetrator

The identity of the offender and victim was known early in the investigation in majority of cases (97.6%). The perpetrator disclosed their guilt in 36.6% of cases, and took their own life in 24.3% where it was evident that they were responsible for the murder. This is consistent with the immediate identification of the perpetrator in the majority of domestic violence homicides where they are often

arrested at the scene and admit their guilt (Kellerman & Mercy, 1992). In such cases and where there is sufficient evidence to support a prosecution, there may not be any requirement for more detailed investigation (Centrex, 2006). This will influence related levels of resourcing, including the degree to which digital devices attributable to the victim or perpetrator are examined (Rogers et al., 2007).

Based on this, 60.9% of the cases would not have required significant investigation of the circumstances leading up to the homicide in order for the Senior Investigating Officer (SIO) to comply with the requirements of the Murder Investigation Manual (Centrex, 2006). The circumstances of the remaining 14 cases also clearly met the definition of a Category C investigation[4] (Centrex, 2006) and were also unlikely to involve examination of digital devices, enabling evidence of cyberstalking to potentially remain hidden. There were two cases (D10 and D19) which required a deeper level of investigation due to problems locating the body of the victim or where the perpetrator initially denied responsibility. It is interesting, therefore, that a more thorough investigation in both cases presented substantial evidence of cyberstalking.

This suggests that the need to establish evidence of the use of technology and cyberstalking in order to prove the guilt of a perpetrator may not be necessary in many cases where domestic homicide occurs. However, it does suggest the importance of early intervention and the collection of relevant digital and other evidence when investigating domestic violence cases in order to ensure effective risk assessment, prosecution of perpetrators and the safeguarding of victims from future escalation. It also highlights the need for the DHR process to consider whether evidence of stalking and cyberstalking was missed in order to ensure that there is effective organisational learning around the potential involvement of these behaviours in domestic homicide.

[4] A homicide is classified as category C where the identity of the perpetrator is known at the outset and related investigation and evidence collection is easily achieved (Centrex, 2006).

Behavioural and Psychological Indicators

The analysis identified clear evidence of behavioural and psychological indicators of stalking and cyberstalking during or after the relationship between the victim and perpetrator. A number of different risk indicators for domestic violence and homicide were identified in the DHR analysis. There was evidence of a controlling relationship on the part of the perpetrator in 63.4% of cases.

> The victim, according to agency records, reported that the perpetrator would often attempt to stop her seeing or calling family or friends by confiscating her mobile and keeping her within the accommodation at the time. (D8)

> The perpetrator changed when they were married. Her Facebook page was closed, and when she was with friends he would call her. (D36)

There was also evidence that the victim had separated, or was intending to separate, from their abuser in 68.3% of cases.

> The victim… went to the home address of the perpetrator. It is believed that she had agreed to see him with the intention of ending their relationship. (D4)

> The victim told the officers that her marriage to the perpetrator was over but he would not accept this. (D28)

There was also evidence of paranoia on the part of the perpetrators in 22.0% of cases.

> The alleged perpetrator thought that the police were following him because he was not going to work, that he would be arrested and therefore he would make detours in journeys. He took to wearing his coat indoors as he felt safer. (D5)

> There were examples of the perpetrator becoming paranoid about what the victim was getting up to, expressing jealousy and seeking to control and manage her relationship with others. (D46)

Some cases evidenced combinations of these different behaviours and characteristics, with evidence of control land separation commonly found.

> The victim wanted to end the relationship. She told how the perpetrator was jealous of her and how he wanted to control who and when she saw people. (D46)

Evidence of physical stalking and threatening behaviour by the perpetrator, or use of physical violence by the perpetrator prior to the homicide.

> The victim had described thinking that he had read through her post and followed her. The family members had also encountered the perpetrator watching their homes. (D8)

> Family members described him turning up uninvited when she went out with her friends or family. He would… then place the victim in a position that she was not able to send him away. (D10)

> The victim was visiting (a friend) at her flat when the perpetrator arrived and kicked the door in and came bursting into the flat. He grabbed the victim around the neck and pushed her up against the wall. He then dragged her by the hair into the hallway and then bathroom. (D27)

These results are consistent with the identified role of controlling behaviours in domestic violence and stalking, as well as their involvement in escalation to domestic violence (Stark, 2012; Woodlock, 2017). Many also demonstrated psychological problems and/or dysfunction in the perpetrators (e.g., jealousy, anger, psychopathy), consistent with the existing literature in this area (Hakkanen-Nyholm, 2010; Spitzberg & Veksler, 2007). Evidence that separation or intention to separate was a trigger for escalation of behaviour is also consistent with research suggesting this is a factor precipitating subsequent homicide (Finn & Atkinson, 2009; Stark, 2012). As these behaviours are related to the questions included in the DASH risk assessment (Safelives, 2014), the results suggest that the cases addressed by the DHRs would have been classified as high risk should this have been undertaken prior to the homicide, and earlier intervention may have prevented the subsequent outcome.

Digital Evidence

41.5% of DHRs made no reference to any digital footprint on the part of either perpetrator or victim, whilst 29.2% included elements of digitally enabled monitoring of social media accounts or emails, or

a series of unwanted texts or messages. In the other cases where it was assumed the digital footprint of the victim and/or perpetrator was missed, similar evidence might have been identified had relevant and/or more detailed examination of devices and social media account been undertaken. Overall, the analysis suggested that 58.5% of cases presented some evidence of digital activities or behaviours associated with the case which would constitute cyberstalking.

Evidence of text messaging was found in approximately 36.6% of cases and use of social media in 17.1%, and this was related to surveillance, sending threats and intimidating victims. These behaviours are consistent with risk factors identified in the literature and reflect high risk of domestic violence and homicide in the DASH (Safelives, 2014).

> "The victim told family and friends that she thought that the perpetrator was accessing her text messages." (D10)

Evidence of account hacking was found in 12.2% of DHRs.

> Her estranged husband became suspicious that she was seeing someone else. Therefore, he "hacked" into her Facebook account. (D10)

> (The perpetrator) stated that … he managed to get into (the victim's) emails and found out she had been communicating with her ex-partner. (D29)

Two cases involved covert recording by the perpetrator, and also involved physical stalking.

> (The perpetrator) often covertly recorded conversations using his computer and a memory stick…The name of the recording had been changed three times in total with the second name change shown as "my last conversation with (the victim)". (D45)

In some cases where physical surveillance was indicated, the perpetrator's knowledge of the victim's movements was unexplained, yet evidence was found elsewhere of potential sources of digital information being available to the perpetrator.

> (The perpetrator) had turned up at a restaurant where she and her mother were dining with friends. He had attempted to establish whether (the victim) was there with a man and had left prior to (the victim) calling the police. He had sent her several text messages saying that he could not live without her. (D28)

In this case, it was unclear how the perpetrator knew where the victim would be. The contact made by text indicates that he had details of her phone, and this raises the possibility that he had installed some form of tracking application on her phone or used her password to access 'find my iPhone' capabilities. This is consistent with the identified availability and use of a variety of spyware and tracking applications available to perpetrators which are designed for locating devices, as well as those with legitimate use for tracking family members and children (Chatterjee et al., 2018; Harkin et al., 2019; Matthews et al., 2017). Although these potential uses of technology were not examined during the investigations or DHR reviews, it suggests that perpetrators' access to digital information about their victims is a potentially important enabler of stalking behaviour, escalation and the subsequent outcome.

Another case provided evidence of a range of digital capabilities on the part of the perpetrator throughout the course of stalking and abusive behaviour. This included access to texts, surveillance of Facebook activity, as well as hacking and impersonation of the victim.

> Unbeknown to (the victim), (the perpetrator) searched her mobile phone and copied all the texts between her and (another party) to his mobile. This took place at least one week before her death. (D45)

Only one case provided direct evidence linking physical stalking and cyberstalking (D10), with evidence that the perpetrator hacked into the victim's accounts, turned up at events the victim attended and considered using electronic tracking devices.

Victims' Digital Vulnerability

Another identified theme related to the ways in which the individual victim's use of social media and technology in their daily lives was intrinsic to their relationship with partners, and this contributed to the digital vulnerability of victims. 17.1% of DHRs made mention of stalking, harassment or the victim's digital vulnerability. One report demonstrated an awareness of online vulnerability through the potential for a perpetrator to monitor the victim's communication. In another, the DHR highlighted that the perpetrator was able to monitor the victim's email and identified that she was in contact with a support agency and intended to leave him. Given that separation has been identified as an important trigger for escalation, this unintentionally increased the risk to the victim.

This suggests that the DHR process itself identified vulnerabilities associated with technologies and online behaviours which are involved in stalking, domestic violence and homicide in some cases. It reinforces the need for strategies which aim to increase victim and general public awareness about the relationship between these behaviours. It is also important to ensure the communication of specific actions that should be taken by those being victimised in this way, as well as related sources of support available (Henry & Powell, 2016; Woodlock, 2017).

Semi-structured Interviews

The behaviours described by the participants in the three cases examined by semi-structured interview were not understood (by victims and parents of victims) as being cyberstalking. One victim considered that she was being stalked but did not make the link to her own digital footprint, and the possibility that this was informing the perpetrator's behaviour. Another accepted that their partner would know where they would be and did not consider whether he had used any digital means to confirm or seek her whereabouts. Despite this, all of the cases demonstrated the involvement of technology and the online environment. The use of text messaging was common in each case, with both victims and perpetrators having access to computers or smart devices and being regular social media users.

Participant 1 had been in a controlling relationship with her abuser which ended when he attacked her with a hammer. Thankfully she escaped before he could kill her, so these circumstances were never examined in a DHR. Thus her interview gave unique insight from the surviving victim's perspective that cannot be provided in a DHR. Her perpetrator stalked her and others for several years after their separation. She describes him as initially 'computer illiterate', but text messaging nevertheless formed an integral part of his early stalking. This indicates that a high level of technical sophistication is not required to engage in cyberstalking behaviours.

> He was ringing me, he was texting me, he was still making threats to commit suicide … but you know, it was just everywhere I went, he was there. (P1, stalking victim)

Participant 1's abuser was subsequently jailed for breaching restraining orders, after which he strengthened his effort by combining elements of cyberstalking.

> But what I think is really relevant is that this man … he was completely computer illiterate – he didn't use a computer at all. But …as part of his rehabilitation process he'd been sent on a computer course… And so I think, you know, online activity just gives you the perfect platform for that kind of predatory behaviour. (P1, stalking victim)

Participant 2 was the parent of a woman killed by her partner who was already standing trial for a series of rapes and assaults against her. He murdered her before those cases came to trial. However, this incident pre-dates the introduction of DHRs and so was not subject of any such formal review. The parent's account therefore provides another unique insight not available through analysis of DHRs. Again, text messaging was a common means of exerting control.

> He used to text her and call her multiple times during the day and you know, she'd say where she was… One of his messages was "get together, we get married or else." (P2, Parent of murder victim)

The perpetrator in this case also had their own digital capability and again made use of social media.

> He had multiple mobile phones… but we do know from court… that he was able to access her Facebook account… he was monitoring her posts, he seemed to know exactly where she was… (P2, Parent of murder victim)

Participant 3 was another parent of a murder victim, and the case was the subject of a DHR. Although not one of the 41 selected for this research, for comparative purposes it was examined retrospectively. Control of the victim through text messaging was again prevalent and identified in the DHR. The DHR also identified that the perpetrator had controlled and harassed previous victims through extensive text-messaging.

> So he was very manipulative and very controlling in that respect but it was the constant telephoning and the constant texts when he wasn't living with her. She used to have to turn her phone off in the end… she would often wake up in the morning to perhaps 50/60 texts, dozens of missed calls asking her where she was. (P3, Parent of murder victim)

The victim also had a heavy online presence and used a variety of social media platforms. However, no indication of this was made in the DHR.

> She had a very, very active Facebook page with loads of updates, comments, loads of pictures, loads of friends… She was quite social media savvy and she used social media as a huge tool to communicate with friends and colleagues at work. (P3, Parent of murder victim)

These cases provided clear evidence of the use of text messages and the online environment to monitor and contact victims. This suggests that sending of multiple messages over short periods of time associated with surveillance and / or coercive control are a risk factor for escalation of behaviour, consistent with previous empirical research and the DASH risk assessment (Hardesty et al., 2015; Safelives, 2014; Woodlock, 2017). There was also evidence of the use of physical and technological stalking behaviours by perpetrators, demonstrating an overlap between the two. This suggests that when the use of technology in this way is brought to the attention of the police and other relevant agencies, appropriate action should be taken in response (Henry & Powell, 2016; Woodlock, 2017).

This requires the development and implementation of effective procedures for responding to such situations by police and other agencies.

Law Enforcement Digital Capabilities

There was little direct reference made to the securing of relevant digital evidence in the DHRs, and only one case mentioned the police response to abuse reported on social media.

> He [the police office] did not view any of the Facebook messages or speak to (the victim, the perpetrator or the caller). (D19)

The officer's lack of action may reflect a lack of understanding of the relevant law, and/or relevant methods to secure related evidence of harassment. This indicates a potential lack of understanding in frontline officers about how online offences equate to those which are committed face to face. It is also possible that where an offence is recognised, those frontline officers do not know how to secure relevant evidence if it has been committed online other than by seizing the device itself for forensic examination, which they are reluctant to do so for what may be perceived as 'lower level' offences.

However, reference was made by the interview participants of their experience of police investigations involving digital evidence.

> If any of the clients we support [participant now supports other victims] report anything online to the police, the police clearly haven't got the knowledge or the awareness around the significance of that. (P1, stalking victim)

> It was the murder investigation that brought out the text messages, the Facebook stalking and the physical stalking, he knew where she was. (P2, Parent of murder victim)

> The only time (the police) saw her phone was when …he had bombarded her with text messages and all of that and one of the texts that he sent, it said something like 'if you don't call me now I'm gonna come round and put a baseball bat round your dad's house and smash up your head'. We

> showed that to the officers there and they said, "Well there's nothing you can do about that." (P3, Parent of murder victim)

One case provided evidence of the perpetrator and victim initially meeting online and the perpetrator maintaining an online presence throughout their relationship and of stalking the victim throughout. No mention was made in the DHR of communications between or online activity around either the perpetrator or victim at the time of her death.

> The family believe that (the victim) met (the perpetrator) via an internet social networking site and very quickly he began to isolate (her) from the family. (D9)

> An ex-girlfriend of (the perpetrator) reported to the police that she had received nuisance texts from him and that he had accused her of hacking into his social networking site. (D9)

This suggests that digital evidence is often overlooked in investigations relating to intimate partner abuse where serious violence or homicide has not taken precedence.

Many authors (e.g., Hoolachan and Glisson, 2010; Mislan et al., 2010; Hitchcock et al., 2016) have raised the increasing need for frontline officers (i.e. non-digital forensic specialists) to acquire the capability to effectively handle digital evidence from the point of first response. They suggest this requires clearly defined practices, allocation of resources, training and tool support. There are a number of frameworks which aim to provide such digital forensic clarity and standardisation (e.g., Agarwal et al., 2011; Al-Mutawa et al., 2016). James and Gladyshev (2013, p. 152) suggested that "a non-specialized analyst should be supported, at a minimum, with a specialized-investigator-approved task checklist and decision matrix". Approaches have been proposed to train and empower first responders to collect digital evidence (e.g., James & Gladyshev, 2013; Hitchcock et al., 2016). However, this task is particularly challenging in the context of domestic violence due to the use of sophisticated mechanisms by stalkers, such as spoofed or anonymous text messages (Horsman & Conniss, 2015). It may also involve the use of GPS trackers and stalker spyware including "dual-use apps" (Eterovic-

Soric et al., 2017; Freed et al., 2018). The use of such tools complicates the identification of abusers or even hinder the ability to forensically recover digital evidence from victims' devices. This might suggest to frontline officers and staff that digital evidence should only be handled by experts due to the level of complexity and effort involved. In a murder investigation, the deployment of digital experts would be warranted, but this might not necessarily be the case in more minor cases. If the practitioner dealing with the incident does not considered themselves 'competent', then vital evidence may go unrecorded.

This appears to be the experience of the interview participants in this study. Participant 2 was unaware of any seizure of digital evidence in relation to the multiple rapes and assaults that their daughter had reported prior to her murder. However, the response to the murder itself was thorough.

> It was the murder investigation that brought out the text messages, the Facebook stalking and the physical stalking. (P2, Parent of murder victim)

Participant 3 was more direct. When evidence of threats made by text message were presented while the victim was still alive but being harassed by the perpetrator, they were told by the police that nothing could be done. However, once the murder had taken place every available piece of digital evidence was sought.

Duranti and Endicott-Popovsky (2010) argue that law enforcement agencies need to be forensically ready and programmes are needed that maximise the ability to collect credible digital evidence at minimal cost. The development of on-scene triage processes which utilise digital forensic kiosks for trained first responders is an example of this. Some UK police forces are using these tools (Metropolitan Police, 2017), and it is an aspiration of UK policing to accelerate further development of such capabilities (Scriven & Herdale, 2015). The development of triage tools is an active area of research (e.g., Gentry & Soltys, 2019; Hales & Bayne, 2019; Jusas et al., 2017). However, the use of such resources and further evidence recovery depends on risk assessment of the seriousness of the

offence by the officer in charge (Metropolitan Police, 2017) and their adoption raises challenges. Wilson-Kovacs (2019) examined the use of triage tools in four UK police forces and found that there was a need for clear strategies for conducting technical triage by frontline officers. The study also identified the tension between efficiency, accuracy of results and the reliability of those tools used. This suggests that results from triage need to be considered with caution due to their influence on investigative decision making, and the potentially serious consequences of this for victims of ongoing domestic abuse and violence.

Discussion

This study examined the extent to which there was evidence of the involvement of cyberstalking in domestic homicide cases on the basis of analysis of Domestic Homicide Review (DHR) documents. Three interviews were also conducted with family members of victims of domestic homicide which involved cyberstalking. The overall aim of the study was to develop a deeper understanding of the role of cyberstalking in the escalation of violence to domestic homicide in order to inform further development related to investigative practices, risk assessment and safeguarding procedures.

Investigative and resourcing implications

There was a variety of evidence of the involvement of technology and cyberstalking in the DHRs and interviews analysed by the study. Only one case provided direct evidence linking physical stalking and cyberstalking, although other cases were identified where cyberstalking was implied alongside physical surveillance and/or where there was an indication of a digital footprint for the victim or perpetrator. The fact that technology and cyberstalking was not evidenced in some of the DHRs does not necessarily mean that it was not involved. There was evidence in some DHRs that the digital footprint of the victim and/or perpetrator had not been examined, and this might have provided further relevant evidence had they been investigated.

As discussed previously, the specific characteristics of domestic homicide influence the nature of the police investigation, as well as the extent to which digital evidence is recovered and examined (Centrex, 2006; Rogers et al., 2007; Horsman & Conniss, 2015). As a result, the potential investigative value of digital evidence will vary according to the dynamics of the case, but would be of particular importance in cases where the identity of the suspect is unknown or the perpetrator denies the offence. It is also of evidential value at earlier stages of domestic violence investigations where it can be used to assess risk by identifying threats, coercive control and surveillance which are known to increase risk of escalation of violence and domestic homicide (Dimond et al., 2011; Chatterjee et al., 2018; Freed et al., 2018). An important area for future research would be to examine digital evidence specifically in such cases to identify behavioural indicators of escalation and develop more focused procedures for the recovery and interpretation of relevant digital evidence, as well as to inform the development of risk assessment and investigative strategies (Al Mutawa et al., 2015).

The results of the study did indicate that digital evidence was being overlooked in investigations of domestic violence where serious violence or homicide had not taken precedence. This has implications for policing practice relating to recovery and interpretation of digital evidence, particularly the need to undertake triage of digital evidence when frontline officers attend calls for domestic violence. The current developments in training to provide first responders with the skills and resources to perform these tasks on scene (ACPO, 2012; James and Gladyshev, 2013; Hitchcock et al., 2016; Metropolitan Police, 2017; Wilson-Kovacs, 2019) are important as initial examination of such evidence could further inform completion of risk assessment tools, earlier intervention to prevent escalation and provision of victim support.

Digital vulnerability and gender

Women were victims in 80.5% of the homicides analysed by the study, consistent with the gendered nature of this crime (Monkton-Smith et al., 2014; Home Office, 2018). The results indicated that 5 of

the 8 women responsible for killing their partners (62.5%) had been abused by them prior to the homicide, consistent with escape from chronic abuse being a motivation in these cases (Dermody-Leonard, 1997). None of the cases involving male perpetrators provided any evidence of the victim having been abused. These results are also consistent with the existing literature which examines the role of technology in facilitating the victimisation and harassment of women, as well as stalking (e.g., Henry & Powell, 2016; Eterovic-Soric et al., 2017; Woodlock et al., 2019). This demonstrates that technology is used in this way as part of coercive control and surveillance, and has a facilitating role in domestic homicide. This issue is currently under-recognised and should be more effectively addressed in current risk assessment instruments and police investigations of domestic violence to ensure that the potential use of technology in this way is identified at an earlier stage. This will enable interventions to reduce the ability of perpetrators to monitor victims, and reduce opportunities for them to have access to victim information and activities which have been identified as triggers for domestic homicide (Woodlock et al., 2019). This can also inform the development of interventions and awareness programs to increase victim awareness about the role of technology in surveillance and coercive control, as well as actions and tools which they can use to protect themselves against such behaviours in the cycle of domestic violence and avoid re-victimisation (e.g., Chen et al., 2019; Matthews et al., 2017). Such actions can also incorporate understanding of what works from other forms of victim support and interventions, as well as education and support for perpetrators.

Policy implications

The research suggests that improvements are needed in the collection of digital evidence by frontline officers, together with adaptive change to overcome the existing lack of professional curiosity when dealing with reports of domestic violence and homicide. The DHR process is an important means of driving such change. Currently each local authority reviews the findings of respective DHRs and reports developing themes to the Home Office which, in turn, informs policy making strategies. The

National Violence Against Women and Girls Strategy (UK HM Government, 2016, 2019), and the new Domestic Abuse Bill (2020) promise to ensure statutory guidance is updated so that best practice is embedded and further learning is shared. The last revision of such guidance was in 2016 (UK Home Office, 2016), and there is an opportunity now for the Home Office to refresh these documents and capture the need for DHRs to explore the digital footprints of perpetrators and victims, and to improve understanding of cyberstalking. This can also further inform policing practice and risk assessment, consistent with the objective of ensuring earlier interventions to safeguard victims (UK HMIC, 2019).

A recent review of the DASH risk assessment tool (SafeLives, 2014) identified a number of problems with its use by the police (Robinson et al., 2016). These included a lack of training in how to use the tool, a focus on physical violence and lack of recognition of coercive control which led to an inconsistent use of the DASH by frontline officers in terms of risk classification. This is consistent with the results of other evaluation studies which found that the ability of the DASH to predict domestic homicide and serious physical violence was problematic (Chalkley & Strang, 2017; Thornton, 2017).

A revised version of the DASH was recently piloted in 3 police forces, with evidence suggesting that this led to an improvement of risk classification, particularly in relation to coercive control and stalking (Wire & Myhill, 2018). This included amendments to items related to frequency of within and post relationship surveillance of victims by technology and social media. An important future area for development of risk assessment tools, such as the DASH, would be to incorporate some form of initial triage for digital evidence of surveillance and coercive control on scene. This has also been accompanied by the development of a new joint police and CPS protocol, and checklist which is used to inform decisions whether to proceed with stalking charges (NPCC, 2018). This emphasises the need to gather evidence (e.g., social media messages, phone records, use of tracking applications) when building a case, even in cases where *No Further Action* is taken as an outcome (NPCC, 2018). These

developments, together with the simplification of NPCC guidance on collection of digital evidence and provision of suitably intuitive mobile digital forensic tools for frontline practitioners, are all important in further developing policing capacity in this area. This can empower first responders to provide a professional service to victims of all levels of domestic violence and further facilitate adaptive change in law enforcement (Heifetz & Laurie, 1997; NPCC, 2018).

Evaluation

There were a number of limitations to this study as the DHR dataset used was necessarily selective. Only those in the public domain were used, and the degree to which the available subset was accurately representative cannot be determined. This should be recognised when considering the results and implications of the study. It was also apparent that DHR reports, as a data source, also have limitations. They are based on collaborative review by representatives from all agencies having had contact with the deceased and perpetrator in order to identify lessons to be learnt and improve professional practice (UK Home Office, 2011). As a result, they collate and represent information that is already known. They do not gather fresh information that might help explore new hypotheses. Therefore, if cyberstalking had become evident in the course of the investigation or been made known to one agency before the victim's death, it would be presented. If this behaviour had been present but not discussed by any of the respective agencies this would be absent in the DHR. The supplementary interviews confirmed these limitations and provided useful context. Furthermore, only three interviews were undertaken. Future research would benefit from analysis of a specific and substantial cohort of survivors and witnesses to serious intimate partner violence and homicide.

This study highlights the ability of analysis of DHRs and interviews to develop a deeper understanding of the role of technology in stalking, domestic violence and homicide. Although the study had a relatively small sample size, and is not statistically representative of victims, researchers have argued for the suitability of the use of smaller sample sizes in research of this kind (Bryce et al., 2015; Reid

et al., 2005). The knowledge generated by this study can directly inform evidence-based approaches to policing, service provision and policy making. It can also ensure that the systems implemented are supportive and responsive to the identified needs of the victims of violent crime (Bryce et al., 2015).

Conclusions

This study examined the prevalence of cyberstalking and the role of technology in domestic homicides. It suggests that the digital footprints of victims and perpetrators are often overlooked, preventing a clear understanding of the role of cyberstalking in domestic homicide. The study also demonstrated that this form of offending disproportionately affects women, and locates this issue firmly within current government policy on Violence Against Women and Girls (2018). This highlights the importance of early identification and intervention in ensuring greater protection of vulnerable women and the prevention of domestic homicides.

The existing failures to secure digital evidence are partially the result of the limited obligations placed upon police investigators by the coronary and judicial processes where the guilt of the perpetrator is clear from the outset. It is also in part a result of the lack of professional curiosity, resourcing issues and training gaps for frontline responders and investigators. Existing processes, guidance and technologies in the area of digital forensics present obstacles to frontline staff that prevent the delivery of the requisite adaptive change to raise such professional curiosity and enable the mainstreaming of digital evidence seizure. Change can be brought about through the Ending Violence Against Women and Girls Strategy (HM Government, 2016, 2019), the police service's Authorised Professional Practice for Domestic Abuse (College of Policing, 2015) and the Digital Investigation and Intelligence Strategy (College of Policing, 2017). Greater understanding can also be gained through further research examining digital evidence. Such research would benefit from the examination of a larger cohort of survivors and witnesses to intimate partner homicide and attempted homicide, including, where possible, perpetrators themselves.

References

Agarwal. A., Gupta, M., Gupta, S., and Gupta, S.C., 2011. Systematic digital forensic investigation model. *International journal of computer science and security*, 5 (1), 118-131.

Al Mutawa, N., Bryce, J., Franqueira, V. N. L., and Marrington, A., 2016. Forensic investigation of cyberstalking cases using behavioural evidence analysis. *Digital investigation*, 16, 96-103.

Association of Chief Police Officers, 2012. *ACPO Good practice guide for digital evidence, version 5*. London: Association of chief police officers of England and Wales.

Bjorklund, K., Hakkanen-Nyholm, H., Sheridan, L., and Roberts, K., 2010. Coping with stalking among university students. *Violence and victims*, 25 (3), 395-408.

Bogdan, R. and Biklan, S.K., 2007. *Qualitative research for education: An introduction to theories and methods, 5th Edition*. Cambridge: Pearson.

Bowen, G.A., 2009. Document analysis as a qualitative research method. *Qualitative research journal*, 9 (2), 27-41.

Braun, V., and Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative research in psychology*, 3 (2), 77-101.

Bryce, J., Brooks, M., Robinson, P., Stokes, R., Irving, M., Lowe, M., Graham-Kevan, N., Willan, V.J., Khan, R., and Karwacka, M., 2016. A qualitative examination of engagement with support services by victims of violent crime. *International review of victimology*, 22 (3), 1-17.

Carpenter, C.J., and Spottswood, E.L., 2013. Exploring romantic relationships on social networking sites using the self-expansion model. *Computers in human behaviour*, 29 (4), 1531-1537.

Cavezza, C., and McEwan, T.E., 2014 Cyberstalking versus offline stalking in a forensic sample. *Psychology, crime and law*, 20, 955-970.

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., Mccoy, D., and Ristenpart, T., 2018. The spyware used in intimate partner violence. *IEEE symposium on security and privacy*, 441-458.

Chalkley, R., and Strang, H. 2017. Predicting domestic homicide and serious violence in Dorset. *Cambridge journal of evidenced-based policing*, 1, 81–92.

Centrex, National Centre for Policing Excellence, 2006. *Murder investigation manual*. Wyboston: National Centre for Policing Excellence.

Centrex, National Centre for Policing Excellence, 2008. *National Intelligence Model, Code of Practice*. London: Home Office.

College of Policing, Authorised Professional Practice, 2015. *Authorised professional practice on domestic abuse*. London: Home Office.

College of Policing, Authorised Professional Practice, 2016. *National Decision Model*. College of Policing.

Crowe, J., and Davidson, T.S., 2009. The "grey" intersection of open source information and intelligence. *The grey journal*, 5, 123-133.

Day A. and Bowen E., 2015. Offending competency and coercive control in intimate partner violence, *Aggression and violent behavior*, 20, 62-71.

Dermody-Leonard, E.A., 1997. *Convicted survivors: The imprisonment of battered women who kill*. Available from: http://freebatteredwomen.org/pdfs/convsurv.pdf

Dimond, J.P., Fiesler, C., and Bruckman, A.S., 2011. Domestic violence and information communication technologies. *Interacting with computers*, 23, 413-421.

Domestic Abuse Bill, 2020. [Online] Available from: https://www.gov.uk/government/collections/domestic-abuse-bill

Duggan, M., Rainie L., Smith, A., Funk, C., Lenhart, A., and Madden, M., 2014. *Online harassment*. Pew Research Center. Available from: http://www.pewinternet.org/files/2014/10/PI_OnlineHarassment_102214_pdf.pdf

Duranti, L., and Endicott-Popovsk, Y.B., 2010. Digital records forensics: A new science and academic program for forensics readiness. *Journal of digital forensics, security and law*, 5 (2), 45-57.

Elphinston, R.A., and Noller, P.N., 2011. Time to face it! Facebook intrusion and the implications for romantic jealousy and relationship satisfaction. *Cyberpsychology, behavior, and social networking*, 14 (11), 631-635.

Eterovic-Soric, B., Choo, K-K. R., Ashman, H., and Mubarak, S., 2017. Stalking the stalkers – detecting and deterring stalking behaviours using technology: A review. *Computers & security*, 70, 278-289.

Finn, J., and Atkinson, T., 2009. Promoting the safe and strategic use of technology for victims of intimate partner violence: Evaluation of the technology safety project. *Violence against women*, 15, 1402-14.

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., and Dell, N., 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *CHI '18: Proceedings of the 2018 conference on human factors in computing systems*, 1-13.

Gentry, E. and Soltys, M., 2019. SEAKER: A mobile digital forensics triage device. *Procedia computer science*, 159, 1652-1661.

Hakannen-Nyholm, H., 2010. Stalking. In J. M. Brown and E. A. Campbell (Eds.), *The Cambridge handbook of forensic psychology*. Cambridge: Cambridge University Press.

Hales, G., and Bayne, E., 2019. Investigating visualisation techniques for rapid triage of digital forensic evidence, *In Proceedings of 2019 international conference on human-computer interaction for cybersecurity, privacy and trust*, 277-293.

Hardesty, J. L., Crossman, K. A., Haselschwerdt, M. L., Raffaelli, M., Ogolsky, B. G., and Johnson, M. P., 2015. Toward a standard approach to operationalizing coercive control and classifying violence types. *Journal of marriage and family*, 77 (4), 833-843.

Harkin, D., Molnar, A., and Vowles, E., 2019. The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, media, culture: An international journal*, doi.org/10.1177/1741659018820562

Henry, N., and Powell, A., 2015a. Beyond the 'sext': technology-facilitated sexual violence and harassment against adult women. *Australian & New Zealand journal of criminology*, 48 (1), 104–118.

Hitchcock, B., Le-Khac, N., and Scanlon, M., 2016. Tiered forensic methodology model for digital field triage by non-digital evidence specialists. *Digital investigation*, 16, 75-85.

Home Office, 2011. *Multi-agency statutory guidance for the conduct of domestic homicide reviews*. London: Home Office.

Home Office, 2013a. *Circular: New government domestic violence and abuse definition.* London: Home Office.

Home Office, 2013b. *Domestic homicide reviews: Common themes identified as lessons to be learned*. London: Home Office.

Home Office, 2018. *Crime Survey for England and Wales 2017-8*. London: Home Office.

Hoolachan, S.A., and Glisson, W.B., 2010. Organizational handling of digital evidence. *Proceedings of the conference on digital forensics, security and law, 33-44.*

James, J., and Gladyshev, P., 2013. A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. *Digital investigation*, 10 (2), 148-157.

Jusas, V., Birvinskas, D., and Gahramanov, E., 2017. Methods and tools of digital triage in forensic context: Survey and future directions. *Symmetry*, 9 (49), 1-20.

Kellerman, A.L., and Mercy, J.A., 1992. Men, women and murder: Gender-specific differences in rates of fatal violence and victimization. *The journal of trauma and acute care surgery*, 33 (1), 1-5.

Legislation.Gov.Uk., 1997. Protection from Harassment Act 1997.

Logan, T.K., and Walker, R., 2017. Stalking: A multidimensional framework for assessment and safety planning. *Trauma, violence, & abuse*, 18 (2), 200-222.

Maple, C., Short, E., and Brown, A., 2011. *Cyberstalking in the United Kingdom: An analysis of the Echo pilot survey*. [Online] University of Bedfordshire.

Marcum, C.D., Higgins, G.E., and Nicholson, J., 2016. I'm watching you: Cyberstalking behaviors of university students in romantic relationships. *American journal of criminal justice*, 42 (2), 373–388.

Metropolitan Police Service, 2017. *Freedom of information request on the existence and use of mobile examination/extraction kiosks*. Available at: https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/disclosure_2017/april_2017/information-rights-unit--mobile-phone-data-extraction-carried-out-at-local-police-station-and-hubs. London: Metropolitan Police Service.

Mislan, R.P., Casey, E., and Kessler, G.C., 2010. The growing need for on-scene triage of mobile devices. *Digital investigation*, 6 (3-4), 112-124.

Monckton-Smith, J., Williams, A., and Mullane, F., 2014. *Domestic abuse, homicide and gender*. London: Palgrave MacMillan.

National Police Chief's Council, 2018. *Protocol on the appropriate handling of stalking or harassment offences between the National Police Chiefs' Council and the Crown Prosecution Service*. London: National Police Chiefs' Council and the Crown Prosecution Service.

National Police Chief's Council, 2016. The national policing homicide working group. *Journal of homicide and major investigation*, 11 (1). Sheffield: The National Policing Homicide Working Group.

Perry J., 2012. *Digital stalking: A guide to technology risks for victims*. Lydney: Network for Surviving Stalking and Women's Aid.

Reckdenwald, A., and Parker, K.F., 2010. Understanding gender-specific intimate partner homicide: A theoretical and domestic service-oriented approach. *Journal of criminal justice*, 38 (5), 951–8.

Richards, L., 2003. *Findings from the multi-agency domestic violence murder reviews in London*. London: Metropolitan Police.

Robinson, A., Myhill, A., Wire, J., Roberts, J., and Tilley, N., 2016. *Risk-led policing of domestic abuse and the DASH risk model*. What Works Centre: Crime Reduction Research. London: College of Policing.

Robson, C., 2011. *Real world research*. 3rd Ed. Chichester: Wiley.

Rogers, M., Scarborough, K., Frakes, K., and San Martin, C., 2007. Survey of law enforcement perceptions regarding digital evidence. *In Chapter 3 of advances in digital forensics III, the international federation for information processing*, 242, 41-52.

Roberts, K.A., 2005. Associated characteristics of stalking following the termination of romantic relationships. *Applied psychology in criminal justice*, 1 (1), 15-35.

Safelives, 2014. SafeLives Dash risk checklist for the identification of high risk cases of domestic abuse, stalking and 'honour'-based violence. [Online] Available from: http://safelives.org.uk/sites/default/files/resources/Dash%20%for%20IDVAs%20FINAL.pdf

Scriven, O., and Herdale, G., 2015. *Digital investigation and intelligence: Policing capabilities for a digital age*. London: College of Policing.

Sheridan, L., and Roberts, R., 2011. Key questions to consider in stalking cases. *Behavioral sciences & the law*, 29, 255-270.

Spitzberg, B.H., and Veksler, A.E., 2007. The personality of pursuit: Personality attributions of unwanted pursuers and stalkers. *Violence and victims*, 22 (3), 275-289.

Stark, E., 2012. Looking beyond domestic violence: Policing coercive control. *Journal of police crisis negotiations*, 12, 199-217.

Thornton, S., 2017. Police attempts to predict domestic murder and serious assaults: Is early warning possible yet? *Cambridge journal of evidence-based policing*, doi:10.1007/s41887-017-0011-1

UK HM Government, 2016. *Ending violence against women and girls. Strategy 2016-2020*. London: National Archives, Her Majesty's Government.

UK HMIC, 2014. *Everyone's business: Improving the police response to domestic abuse.* London: Her Majesty's Inspectorate of Constabulary.

UK HMIC, 2019. *The police response to domestic abuse – An update report*. London: Her Majesty's Inspectorate of Constabulary.

Wilson-Kovacs, D., 2019. Effective resource management in digital forensics: An exploratory analysis of triage practices in four English constabularies. *Policing: An international journal of police strategies and management*, 1-14, doi.org/10.1108/PIJPSM-07-2019-0126

Woodlock, D. 2017. The abuse of technology in domestic violence and stalking. *Violence against women*, 23 (5), 584–602.

Woodlock, D., McKenzie, M., Western, D., and Harris, B. 2019. Technology as a weapon in domestic violence: Responding to digital coercive control. *Australian social work*, DOI: 10.1080/0312407X.2019.1607510