'Why Don't You Block Them?' Police Officers' Constructions of the Ideal Victim When Responding to Reports of Interpersonal Cybercrime

BLACK, Alexandra <http://orcid.org/0000-0002-5910-0108>, LUMSDEN, Karen and HADLINGTON, Lee

Published version

BLACK, Alexandra, LUMSDEN, Karen and HADLINGTON, Lee (2019). 'Why Don't You Block Them?' Police Officers' Constructions of the Ideal Victim When Responding to Reports of Interpersonal Cybercrime. In: LUMSDEN, Karen and HARMER, Emily, (eds.) Online Othering. Palgrave Studies in Cybercrime and Cybersecurity . Springer International Publishing, 355-378.

‘Why don’t you block them?’ Police officers’ constructions of the ideal victim when responding to reports of interpersonal cybercrime

Alex Black, Karen Lumsden and Lee Hadlington

Abstract

This chapter explores police officers’ responses to reports of interpersonal cybercrime by considering their construction of the ‘ideal victim’. It also contributes to knowledge on police officers’ perceptions of cybercrime and their support for victims. The discussion draws on Nils Christie’s (1986) concept of the ‘ideal victim’ to explore which individuals police officers most readily give the legitimate status of victim. In order to explore this, three themes are discussed including: police officers’ constructions of the ‘ideal victim’; their attitudes towards victims in relation to prevention of cybercrime (i.e. ‘block them’) and; negotiations over responsibility for dealing with the emerging issue of cybercrime. The chapter argues that police forces must advance beyond an approach which entails victim-blaming and instead recognise the centrality of social media and online spaces in individuals’ lives. Data are presented from focus groups and interviews with police officers and observation of call handlers and dispatchers in a police force control room in England.

Keywords

Cybercrime, internet, online abuse, policing, prevention, social media, victim

Introduction

This chapter focuses on the responses to interpersonal cybercrime victims by police forces in England, drawing on data from focus groups and interviews with police officers, and an

ethnography of a police force control room. The discussion centres on how police officers construct notions of the 'ideal victim' (Christie, 1986) of online crime, how these inform their attitudes towards victims, and how they respond to reports. Importantly, this chapter demonstrates the ways in which the police response at present could be seen to involve victim-blaming by framing online users as making themselves vulnerable to cybercrime through their occupation (and use) of particular virtual spaces. Police officers' suggestions to withdraw from these social spaces (i.e. via police advice to victims to 'just block them' on Facebook) often meets resistance from victims and risks isolating and excluding victims from everyday forms of online interaction (Hadley, 2017).

The emergence and expansion of cybercrime has generated numerous debates and tensions over how it can be defined, what the scale of the problem is, and who should be responsible for dealing with it (Caneppele and Aebi, 2017; Wall, 2008a). Distinctions in the definitions of cybercrime are made between property cybercrime (committed for financial gain) and interpersonal cybercrime (those behaviours aimed at a particular victim) which can blur the boundaries between offline and online victimisation (Burns and Roberts, 2013). For example, online forms of interpersonal abuse are often an extension of, and addition to, offline forms of abuse such as violence and coercive and controlling behaviours (Hadley, 2017). Police services in the UK have not yet adapted to deal with the complexity and volume of interpersonal cybercrime such as online abuse, revenge pornography and domestic incidents (Laville, 2016). The police response to victims of certain forms of interpersonal cybercrime has also been questioned due to their potential for what may be seen as victim-blaming (Jane, 2017a).

This chapter explores police responses and the way in which they draw upon notions of the 'ideal victim' and perceived seriousness of the offence. It then considers how these responses are situated in the sociocultural context of austerity policing. Policing in the UK is currently undergoing substantial changes as a result of the neoliberal context of austerity ushered in post-2008 recession. The government's 2010 spending review enforced a 20 per cent funding reduction to police forces between 2011 and 2015, which amounted to £2.53 billion pounds worth of savings across forces (HMIC, 2014). Police officer and staff reductions accounted for a large proportion of these savings, directly impacting on routine and frontline police work, and fostering low morale amongst staff (Lumsden and Black, 2018). We argue that the increasing volume of cybercrime within an environment of depleted resources leaves officers negotiating with victims over who should primarily take responsibility for dealing with these offences. These negotiations can be seen as part of a broader opportunity to re-define and narrow what 'post-austerity policing' will look like (Millie, 2014). Certain forms of interpersonal cybercrime did not elicit 'ideal victim' status from officers, for example domestic incidents taking place on social media in which the victim did not remove themselves from the online environment. This was distinct from 'ideal victims' who were more easily considered a blameless victim of an anonymous cyber-criminal. The absence of 'ideal victim' status for certain interpersonal forms of cybercrime contributes to officers' debates over whether to include these offences as a priority in a renegotiated policing landscape. The chapter proposes that a substantial reframing of police support for victims of online crime is urgently required, in order to recognize the serious ramifications of online hate, cyber-stalking, and technologically-mediated domestic abuse, and to go beyond commonsensical assumptions that victimization in 'the virtual world' is less serious or impactful than it is in relation to traditional offline crimes. It further argues that this

online/offline dichotomy must be challenged so that police and agencies can effectively support victims of cybercrime.

The chapter begins with an overview of the definitions and emergence of cybercrime and the policing response to it. It then discusses key terms and ideas within the field of victimology; in particular Christie's (1986) concepts of the 'ideal victim' and the deserving and undeserving victim, and how these apply in the cybercrime context. After outlining methods, the chapter presents findings including: police constructions of the ideal victim; police responses to interpersonal cybercrime and advice for managing victimisation; and police negotiations over responsibilising individuals for managing online risk.

Review of literature: cybercrime, victimisation and the police response

Defining and policing cybercrime

The topic of cybercrime has become a critical focus for many, including researchers, law enforcement, and those developing government policies. However, despite the overwhelming interest in the area of cybercrime, it lacks a universally accepted definition (Gordon and Ford, 2006; McQuade, 2007). This lack of agreement regarding the definition of cybercrime has in turn been linked to widespread confusion about the actions and behaviours that fall into the category (Wall, 2008a; Wall, 2008b). The term is often used to describe crimes involving computers (McQuade, 2007), but can be used to refer to a much broader set of crimes. Researchers have moved away from the use of cybercrime as a term that just refers to the use of the internet to commit crime, in favour of viewing it in terms of a continuum (Gordon and Ford, 2006). This can range from aspects of 'technological crime' (also referred to as cyber-dependent crime) that can only exist within a system such as the internet, or hardware and software. At the other end of the spectrum is 'people crime' (or cyber-enabled crime), in

which technology or the use of the internet is only a minor part of the crime (National Crime Agency, 2016).

Holt et al. (2015) note that the use of the term 'cybercrime' has evolved to describe most criminal activity in the online digital environment. There is a subtle distinction between the two concepts of 'abuse' and 'misuse' in the context of cyber-related activities. Therefore, they use the term 'cyberdeviance' to conceptualise those activities which are not necessarily illegal but can be seen to contravene societal norms and values. This could, for example, include the use of a smartphone in a cinema or theatre during the production. Whilst there is no illegal activity being engaged in (unless the individual is contravening potential copyright laws), they are generally frowned upon by the wider society. Further examples include the viewing of online pornographic images, or sending explicit sex messages (sexting). Neither of these activities are illegal as long as the parties involved are over the age of consent for the particular country (Mitchell et al., 2012). Accordingly, Holt et al. (2015) suggest that the point at which a deviant cyber-related activity becomes 'criminal' is the point at which it transgresses what is 'legal' for that particular country. This also relates to the geo-political landscape for law enforcement of cybercrime.

Researchers have noted that there is little consistency in the policing of criminal activities which involve digital technology (Holt et al., 2015; Wall, 2001; Brenner, 2008). Wall (2001) notes that this issue is related to the concept of *nullen crimen sine lege* (or no crime without law). If a particular country does not have laws in place to tackle a specific aspect of cyber-deviant activity, the legality of such cannot be assessed. Where countries engage in the facilitation of information sharing in the context of multi-national agencies tasked with tackling cybercrimes, these are only effective if the activities under investigation are given

the same weight by each of the member states (Wall, 2001). New forms of online criminality also require amendments to, or additional forms of legislation for police officers to be able to deal with them. This includes, for example, the introduction of a new law in the UK in 2014 to enable prosecution of 'revenge porn' (an offence where people maliciously share sexually explicit pictures of former partners). This problem is in addition to the sheer volume of cybercrime offences that police officers are expected to respond to on a daily basis. As one Chief Constable commented in relation to online abuse: 'The levels of abuse that now take place within the internet are on a level we never really expected. If we did try to deal with all of it we would clearly be swamped' (cited in Laville, 2016).

Defining and policing interpersonal cybercrime

As noted above, cybercrime is generally split into two broad categories of 'interpersonal cybercrime' which involves a personal attack on a victim and 'property cybercrime' which primarily involves financial gain (Burns and Roberts, 2013). The advancements of the internet and communication technologies have allowed interpersonal forms of criminality to 'go viral' and for certain individuals to exploit the online environment to commit acts such as cyber-bullying, cyber-intimate partner abuse, cyber-stalking and cyber-harassment (Navarro and Clevenger, 2017). The quality of the police response to such forms of interpersonal cyber criminality have been called in to question, not only due to of a lack of resources and expertise to deal with these crime reports, but also due to the police-victim interaction that takes place and the level of support provided to victims. Jane (2017b) highlights how police officers can often fail to act in response to interpersonal online victimisation and instead put pressure on victims to withdraw from these online spaces by deleting accounts and changing their phone number. In these instances it is the victim who is responsibilised to deal with and resolve the cyber threat by closing down their accounts. However, this request by the police

that individual victims should remove themselves from cyber spaces fails to acknowledge how integral the online environment is to people's modern day lives and is a response which places blame and responsibility with the victim. The use of the internet, especially for younger generations, is an ‘established fact’ and withdrawal from these spaces has become an unrealistic expectation (Hadley, 2017: 9). The requirement to withdraw can also be seen as a victim ‘punishment’ in that the victim themselves become the excluded party (Jane, 2017a).

There is also reliance on the victim, rather than police investigators, to prove the intent and credibility of the interpersonal offences being reported. This form of victim treatment can often be the result of a lack of legislative knowledge on behalf of the police over what constitutes interpersonal cybercrime (Wall, 2001; Jane, 2017b). There is also evidence to suggest that lower level forms of interpersonal cybercrime are taken less seriously by the police (Bossler & Holt, 2012). Yar (2013) details how our social and cultural judgements around risk, harm and seriousness determine where in a 'hierarchy of standing' a particular crime will be placed by police. These judgements are based on the supposed vulnerability of the victim involved, the dangerousness of the offender in question, the immediacy of the police response, and the physical and/or emotional harm caused to the victim. In this sociocultural context, Yar argues, internet offences such as child pornography are placed at the top of this hierarchy of standing. They are then responded to with the full weight of traditional forms of state-centred public policing. This is in contrast to other forms of cyber criminality where the victim is seen as less vulnerable and less in danger of harm, for example internet 'piracy'. These forms of criminality, that are lower down the hierarchy of standing, are policed less by state-centred agencies and more so by non-state actors such as members of the public, private organisations (such as internet providers) and volunteers.

Responsibility for crime control and self-protection is then shared amongst this network of crime control governance (ibid).

Research also suggests that police officers do not necessarily feel best placed to take responsibility for responding to cybercrime. A survey of response officers in the US conducted by Bossler and Holt (2012: 174) found that officers' main suggestion for how best to respond to the increasing issue of cybercrime was for users to 'be more careful while on line', followed by calls for greater education for users in online safety. This could be seen as a negotiation point in 'responsibilising' individuals in the 'privatisation of risk-management' (Duggan and Heap, 2014: 26) within the context of this emerging crime type. However, the responsibilising of victims may overlook the blurred boundaries and intersections between online and offline offending that occur in many forms of interpersonal cybercrime. Online abuse can be an extension of offline abuse, especially in domestic abuse situations. For a victim to self-police and restrict their online presence, may further exclude and isolate them (Hadley, 2017). Arguments have also been made that the trend towards misogynistic forms of interpersonal cybercrime (including 'revenge pornography', rape threats, and death threats) have a strong silencing effect on women specifically in online spaces and communities, pushing them to withdraw from these spaces (Lumsden and Morgan, 2017; Hadley, 2017; Jane, 2017a). With these complexities in mind it is pertinent to understand how police officers respond to reports of interpersonal cybercrime, how victims are advised and supported, and to consider which forms of cyber criminality generate full 'victim status' from responding officers.

Victimology and the 'ideal victim'

The notion of placing partial responsibility for victimisation on the victim themselves developed in early work in the field of victimology. This work saw the emergence of victim typologies, most notably in the work of Mendelsohn and the notion of victim culpability and Von Hentig's typology of victim proneness (McGarry and Walklate, 2015). Both typologies focused on the role of the victim within offending behaviour and, as McGarry and Walklate argue, also focus on the extent to which the victim had made choices that led to their ultimate victimisation. Mendelsohn and Von Hentig sought to distinguish between victim identity (personal characteristics and vulnerability) and the situational context of an offence (provocation, engaging in criminality, relationship with the offender etc.) which when combined together establish how culpable or blameworthy a victim could be seen to be and thus how deserving they were of victim status. Understanding the 'deservedness' of this victim status highlights how certain victims are viewed and responded to differently in certain situations and the uneven application of the victim identity (Duggan and Heap, 2014). Analysing victimisation through the frame of culpability and proneness placed undue blame on the victim and removed the responsibility for offending away from the offender, ushering in a culture of victim-blaming that still persists today (Cross et al., 2018).

The notion of the deserving and conversely the undeserving victim has been highlighted most clearly in Nils Christie's (1986) notion of the 'ideal victim', a set of characteristics that personify society's expectations over victimhood. Christie sought to emphasise how and in what circumstances some victims were legitimated as deserving of sympathy and others were not. In Christie's typology, an 'ideal victim' is physically weaker than the offender, is unknown to the offender, is unambiguously blameless and is engaged in legitimate activities wherein they were targeted by a 'big and bad' offender. Any individual who meets these criteria is afforded the full weight of victim status and the corresponding support of

responding agencies and the public. Any transgression of these characteristics challenges the application of this status. Christie's concept of the 'ideal victim' has been widely utilised in studies of victims and victimology since its publication and has been applied to our understanding of critical issues including victims of international crimes (van Wijk, 2013), victims of child sexual abuse (McAlinden, 2014) and most recently victims of hacking and data breech (Cross et al., 2018). Christie's work has also been used to understand the construction of the 'ideal victim' in the media (Greer, 2007) and how crime victims self-present their status (Jagervi, 2014). However, thus far there is scarce work exploring how it relates to cybercrime (although see Jane, 2017a; Hadley, 2017), including interpersonal cybercrime or how police responses to cybercrime involve notions of the ideal victim.

Methods

The data presented below is drawn from two qualitative studies of the police response to victims and perceptions of cybercrime. The studies were conducted within one year of each other at two police forces in England.

The first project (Study 1) was an ethnographic study of a police force control room (FCR) in England (see Lumsden and Black, 2018).[1] The study was more broadly concerned with the police response to domestic violence calls at the frontline, which included call handling, dispatch and response officers. 66 hours of observation were conducted between November 2016 and February 2017. This involved a combination of day (7) and early evening shifts (6). Author 1 conducted 11 hours of observation while Author 2 conducted the majority of the observations totalling 55 hours. Ethnography allows for detailed investigation of human behaviour and the factors that influence such behaviour (Brewer, 2000). We participated in the setting by listening to the calls and observing call handler and dispatch behaviours. We

also conducted four focus groups with frontline officers (26 in total) in order to explore their response to domestic abuse calls, and the relationship and interactions between dispatchers in the FCR and frontline officers. The focus groups were audio recorded and transcribed by an independent transcription company. Access to the FCR was granted via the manager who acted as gatekeeper and made decisions as to which individuals or teams we would sit with. We were given a head-set in order to listen to the call handlers and the dispatchers' conversations with response officers and other parties. Short-hand notes of observations and conversations with staff were made in the FCR, either in a notebook or in a mobile phone notes function. This helped to highlight items that we did not want to forget without being intrusive. Field notes were then written up after each observation and described the setting, calls, conversations and incidents.

The second study (Study 2) focused more specifically on frontline police officers' views and perceptions of cybercrime. In total 16 police officers were recruited by a senior police officer based at a Force Headquarters to take part in four focus groups conducted by Author 1 and Author 3. Each officer had a minimum of 18 months service and they were recruited from a variety of operational backgrounds. The breakdown of the focus groups according to operational background is presented in Table 1 below. 4 people were present in each focus group, and these were conducted in gender homogenous fashion with each focus group lasting for approximately one hour. The focus groups were all audio recorded and fully transcribed by an independent transcription company.

Focus group	**Participants' operational background**
Focus Group 1 (Female)	Control Room Operations (x2), Incident Response, Investigations Management Unit

Focus Group 2 (Male)	Control Room Operations (x2), Investigations Management Unit, Control Room Organisation Team
Focus Group 3 (Female)	Investigations Management Unit, Call Management Team, Managed Appointment Unit (x2)
Focus Group 4 (Male)	Managed Appointment Unit[2], Patrol and Resolution Officer, Investigation Management Unit (x2)

Table 1: Focus group break down according to operational background.

In both studies we adopted an iterative-inductive approach to analysis and entered into an ongoing simultaneous process of deduction and induction, of theory building, and testing (O'Reilly, 2005). In this approach theory is developed out of data analysis, and subsequent data collection is guided by the emergent theory. Thematic analysis (see Braun and Clarke, 2006) was utilised to analyse data collected in both studies and adopting an iterative-inductive approach in the first study meant that unanticipated themes, such as those discussed here relating to interpersonal cyber-crime, the response to victims of these crimes, and the relationship between social media abuse and domestic abuse offences, emerged through our analysis. All three authors were involved in the process of data analysis for Study 2, while Authors 1 and 2 analysed the data from Study 1.

Both studies received ethical clearance from the respective universities. Participant numbers and/or pseudonyms have been used to disguise the identities of police officers, staff and callers. The police forces and geographical areas have also been anonymised and any identifying factors omitted from field notes so that they do not result in the identification of the forces or employees.

Results: police officer support for victims of cybercrime

1. The 'genuine' victim of cybercrime

In focus groups, police officers across all departments (including frontline officers and call handlers) constructed notions of what they believed to be the 'ideal victim' or 'genuine victim' of cyber-crime, in contrast to those individuals who they felt had not taken preventative measures to address cybercrime particularly at the interpersonal level (we explore this theme – of 'block them' further below). The police officer below outlines the genuine victim as someone who is already 'vulnerable' in society and who is therefore an easy target for cyber criminals:

> Respondent 1: *... you have ... the really vulnerable people in society that get taken advantage of, especially by social media and on some of these faceless crimes as well and get encouraged to do things that they really shouldn't be doing. So even though I said my empathy levels are low when you start talking to some of these people it goes up quite rapidly. Because you think, crikey, they are really being taken advantage of.*
>
> (Focus group 3, Study 2)

The idea of the 'faceless' criminal operating across the internet fits the popular characterisation in academic and popular literature of cybercrime as anonymously enacted in a distant and unknown cyberspace (Lusthaus and Varese, 2017). This type of criminality allows officers to consider the victim as unambiguously blameless as the offender is unknown and the victim would have been unable to prevent it occurring. These notions of the genuine victim should be seen in context of what officers understand 'proper' cybercrime to be, which mostly characterises property cybercrime, even though many of the cybercrimes reportedly dealt with by officers were interpersonal:

> Respondent 1: *I always just think of internet and I think of faceless people. You know, you've got that computer screen but – and I think that's one of the frightening things, that you don't know who you're dealing with half the time. I know the other things we've mentioned about Facebook harassment are cyber, but to me it's more the faceless side of the internet, when they target people. That's what springs to my mind first of all.*
>
> (Focus group 3, Study 2)

Those online offences that are more interpersonal in nature are more likely to imply that the victim and the offender are known to each other, and thus it is viewed that there are more opportunities for the victim to disassociate from the offender, as can be seen in the quote below:

> Respondent 4: *Yeah, there's a perception from the public that it's cybercrime, definitely, not from the police, I wouldn't have said. It's an open forum where, you know, if you leave yourself open to that sort of thing, and quite often they have their friends on Facebook as opposed to some anonymous person, then, you know, they're allowing that person – you know what I mean, in the first place, they're allowing them to be able to do that because they've friended them and said – then they slag them off, you know.*
>
> (Focus group 6, Study 2)

As can be seen above, distinctions are made between the 'anonymous' offender and the Facebook 'friend'. Facebook in particular was seen as a domain in which the victim has

autonomy over limiting their potential for victimisation by their ability to remove themselves from the platform, even in the context of domestic abuse situations:

> *Dispatcher 17 said that they get a lot of Facebook message related domestic abuse incidents. She said "Facebook domestics make us want to shoot ourselves". I asked why and she intimated that it was trivial. She said that people can block exs or that they can come off Facebook. She said that when she was a call handler before she became a dispatcher she would get a large number of people complaining about messages from people over Facebook or about people posting messages or photos of them on Facebook. She said that this was a typical DA incident…She described herself as losing patience with the callers in her manner with them.*
>
> (Fieldnotes 8th December 2016, Study 1).

As can be seen above, to not disengage is viewed by this call handler as leaving victims 'open' to abusive situations. This view is echoed by the below police officer, who refers to genuine victims as those individuals who have been exploited. Lower level cybercrime is seen as occurring because individuals have not taken preventative measures to protect themselves from harm online:

> Respondent 2: *Yeah, we have genuine victims who just didn't see it coming or who have been blatantly exploited, but then we also have the lower-level stuff which is just down to social irresponsibility and people not taking responsibility for their own actions online. And we have everything from, "Oh, she called me a bitch," and whenever we get a crime report through for that, from – right through to the old dears who've just been sending money to people, massively exploited to high value as well.*

We are constantly fighting against the companies to try and get them on board and help us out with these enquiries. It's extremely difficult.

(Focus group 4, Study 2)

We can see in the quote above how the respondent constructs these two types of victims as on opposing ends of a scale of victimisation, from irresponsible users to exploited 'old dears'. The construction of the ideal victim here strongly echoes Christie's (1986) example of the defenceless elderly woman and the unknown offender. However, it also raises questions of how serious police officers take the offences which they deem to be at the lower end of victimisation. For this next respondent, lower level cybercrime is seen as a lower police priority. Here we can see the sociocultural context of austerity and reduced resources impacting on where in the 'hierarchy of standing' (Yar, 2013) the offences are placed:

Respondent 4: … *as a force, I don't know, as a police service, I think that we pander too much to that low-level cyber aspect of it and something needs to be done otherwise it's just going to be – obviously with the way things are going, our diaries are made up with these…*

Respondent 3: *We're struggling.*

Respondent 4: *... and ... actually the jobs that require more attention, we're not dealing with them because we're dealing with the he said, she said kind of aspects of these kind of things that people have an option to pull out of or to just block or to – and nobody seems to be taking those reasonable steps. And they just – there's the expectation that police will come in and arrest them and sort it out, but we just haven't got that ability and the resources like we probably – well, a few years ago it*

wasn't like this, was it? But, you know, it's – I think there's that expectation that we're going to be doing something about it.

(Focus group 5, Study 2)

In the above quote we see the officers navigate the interrelationship of victim culpability, the perceived seriousness of the offence, and the current context of austerity. In particular, interpersonal types of offences ('the he said, she said') where people can 'pull out' of the situation are seen as diverting resources from more serious and warranted offences. What can be seen here are negotiations over the responsibility for dealing with these new forms of criminality within this reduced resource context. The seriousness of the offence and the 'ideal type' of victim act as anchor points to shape this discussion.

2. 'Have you blocked them yet?': preventing cybercrime

Police officers demonstrated an acute awareness of the centrality of social media in people's daily lives. They also recognised that their typical advice to victims of removing themselves from these platforms was not necessarily victim centred:

Respondent 4: *That, about not taking it seriously, sort of until really the [particular incident] thing if kids said, "I'm being harassed on Facebook, blah, blah, blah," we just said, "Oh well, come off Facebook then." We didn't take that seriously, did we, I think?*

(Focus group 3, Study 2)

However, officers still demonstrated that what they perceived as elements of victim culpability in these interpersonal cybercrime offences shaped their attitudes about the victims and their victim status:

> Respondent 4: *There's a sense of, well, they shouldn't be talking to me like that. No, they shouldn't be, however, you're not taking the bull by the horns and you're not doing anything to stop it yourself. "Why should I?" is the classic. "Why should I?" because – but—*
>
> Respondent 1: *And whenever you do suggest it that they come up with a reason why they shouldn't. "Well, I need to get in touch with so and so, so and so's sister," and you just think, "Well, privacy settings are there for a reason, set them," and they don't. People don't do it.*
>
> (Focus group 5, Study 2)

This description of officers' attitudes towards the victims is not to assert that their response or behaviour towards them was affected, however we do see that the police advice remains the same, even in the face of resistance from the victim. The victim may see the advice from the officers as unjust or victim 'punishment' (Jane, 2017a). This then creates an impasse in the dialogue between the officer and the victim, which impacts the officer's empathy for the victim. As can be seen in the quote below, this same frustration emerges even within domestic abuse situations:

> Respondent 3: *... it's hard to safeguard someone ... I had a domestic harassment and I said to her like, "Why not just stop using Facebook or block him?"*
>
> Respondent 2: *Block them.*

Respondent 3: *And people are so reluctant to do that.*

Respondent 4: *Change their number.*

Respondent 3: *Like they can't see their life past Facebook. And the longer, like eventually she blocked him and we stopped the harassment, so because the harassment stopped, she unblocked him.*

Respondent 4: *People say, "Well I keep it open, I haven't blocked his number because then I won't have evidence that he's harassing me." And it's like, "Well, you won't be harassed if you…"*

Respondent 5: *Yeah.*

Respondent 3: *Can be a little bit frustrating with social media.*

(Focus group 1, Study 1)

This above discussion between response officers is characteristic of Hadley's (2017) assertion that in the context of domestic abuse situations, telling victims to exclude themselves is an inadequate and potentially 'victim-blaming' response. Online abuse can be an extension of offline abuse which, if encouraged to withdraw from these spaces, can further the isolation of victims as a means of coercion and control. Making the victim responsible for blocking the offender to end the harassment may fail to address the actual behaviours of the offender. As the discussion above continued, the officers acknowledged the role of the offender in these situations, but the victim is still seen as responsible for playing a particular role in reducing these forms of criminality themselves:

Respondent 2: *Yeah, we give them like safety advice and words of advice in terms of what they need to do and stuff like that, but it's whether people choose to – you know. We've all – I think everybody's had some victim that said, "I don't want to block them*

because…" and it's like you're saying to them, you know, you can help yourself as well, you know. We can obviously – we definitely go and speak with this person and potentially prosecute them for harassment, but at the same time they're like, "Oh, I don't want to block them because I don't want to lose my amount of friends on – my Facebook friend numbers," and, you know, it's an interesting mind set.

Respondent 4: *Or I want evidence there or I shouldn't have to.*

Respondent 1: *Or it's … "Change your phone number." "Why should I? I haven't done anything."*

(Focus group 1, Study 1)

These same narratives concerning their negotiations with individuals about taking responsibility appear again here. The resistance of members of the public to the police advice that they should block other users on social media, adds to the officer's frustrations and potentially undermines their acknowledgement of the centrality of social media and information and communication technologies in people's lives.

3. Negotiating responsibility for cybercrime

As previously noted, the expansion of cybercrime has increased the workload for police officers (Laville, 2016). Millie (2014) has noted that the post-austerity policing landscape has created uncertainty regarding what the police role should look like. This is due to their reduced resources and amplified democratic accountability over an increasingly wider policing remit. Austerity offers the opportunity for police officers to 'narrow' the focus of policing (Millie, 2014). In the discussion of interpersonal cybercrime, police officers demonstrate engaging in this narrowing of roles by negotiating where the responsibility

should fall for managing these cyber offences, specifically those that do not easily elicit victim status and those they deem to be of a less serious nature.

As can be seen below, the police do not see themselves as primary responders to interpersonal cybercrime. The victim and then the social media company are placed in positions of responsibility before the police:

> Interviewer: *Are they difficult to respond to then, the online-based kind of incidents?*
>
> Respondent 14: *Well you just give the same advice, block them, delete it, you know, etc., and whether they do or not, you have to go on their say-so on that, but—*
>
> Respondent 20: *I think as well it's like, yes, we can be called, however, people – people just don't take a little bit of self-responsibility with stuff. You know, Facebook as an organisation have their processes. They, you know, but no-one – the amount of people I say, "Have you reported it to Facebook you know, so they can look into it, block it, deal with it?" "No." "But you've called the police straight away? Doesn't that seem like you've jumped a few steps there potentially?" And they're like, "No."*
>
> Respondent 14: *I think as well you find with victims that they need to take a little bit more responsibility of themselves.*
>
> (Focus group 3, Study 1)

Other organisations were seen as having pushed responsibility on to the police for dealing with cybercrimes:

> Respondent 3*: When you were at school, when I was at school, if somebody was bullied, school would deal with it, parents were probably brought in, three parties,*

between them probably resolve it. Now the school's washed their hands of anything that's cyber-related or social media-related, they'll go, "Oh, we'll speak to the police." So the schools are not then taking – it might be going on in the school, it's two kids in the same class, but they don't – they wash their hands of it and say, "Contact the police," and that's—

(Focus group 4, Study 2)

As can be seen above, the officers viewed themselves as filling a gap that schools have left open by refusing to respond to offences such as cyber-bullying. For police officers, these offences are an addition to the existing and increasing workload of police teams. Where children are concerned, this then adds to the amount of time taken to deal with these offences:

Respondent 4: *These tiny little jobs actually are – I'm sorry to say, quite meaningless in the grand scheme of things, just have so much ramifications to everything else because when they involve kids you've got the vulnerable person report, that then the vulnerable person's team then get clogged up with all these crap, you know, because—*

Respondent 3: *Social media.*

Respondent 4*: Because of social media, and everybody does it and the parents often don't know what's – sometimes no fault for the parents, but they don't know what they're up to, and it's just – it's an absolute minefield that I think that somebody's got to draw the line somewhere…*

(Focus group 5, Study 2)

The above quote highlights how the officers are trying to re-establish the boundaries of their work. Parents are viewed as being in a position to manage some of what officers perceive to be less serious offences. There is a need to 'draw the line' over what is considered within the police remit and what is not, with a view to a ‘narrowing of focus’ for police work (Millie, 2014). This negotiation, in combination with the 'hierarchy of standing' for less serious offences was seen to add to the frustration and stresses that police officers faced in an austerity climate. The police officers interviewed are in a position where they feel as though they have to prioritise certain offences over others. This pressure positions offences against one another on this hierarchy, potentially adding to the resistance of officers to particular interpersonal cyber-related offences:

> Respondent 1: *That’s occurring more and more because certainly as time goes on and resources for policing becomes less and less, which it is going to continue getting more and more restricted, we are going to get to a point where we’re going to have to turn around and say, “As the police, we no longer deal with this, this and this.” And if it’s a choice between we’ll either deal with your Facebook squabbles or we’ll deal with the actual physical assaults, which would you prefer? And that’s what’s happening. You know, we are getting to a point where officers are sent on grade one responses to turn up to be nasty threats online, yet somebody’s had their house burgled and having to wait two days for us to attend, and I kind of think, “Well, I know which one I should be going to.”*
>
> (Focus group 6, Study 2)

In the above quote, we see the officer position online abuse in opposition to offline offences and in direct competition for resources. Framing offline and online interpersonal crime as a

zero sum game creates tensions within policing and adds to the understanding of who is and is not an 'ideal' victim. This practice allows officers to engage in the ‘othering’ of victims who they perceive as not having achieved true victim status.

Discussion and conclusion

This chapter has demonstrated the way in which officers understand and respond to interpersonal cybercrime. Officers make a distinction between deserving and undeserving victims of cybercrime depending on the level of victim culpability, in particular, their ability to remove themselves from the risk of initial and ongoing victimisation. Drawing on the work of Christie (1986) and the notion of the 'ideal' victim it can be seen how officers construct their understanding of who is an 'ideal' victim. These notions are informed by popular characterisations of cybercrime as anonymous and faceless and occurring in an unknown cyberspace (Lusthaus and Varese, 2017). These forms of cybercrime, which are mostly property related, allow the offender to be 'big and bad' and position the victim as unknowing and blameless, giving them unquestioning victim status. On the other hand, interpersonal forms of cybercrime generally imply a relationship of some sort between the victim and the offender, for example in the case of domestic abuse or ‘revenge pornography’ which then complicates this status. This was especially the case when coupled with what officers denoted as lower level forms of offending which were placed at the lower end of the ‘hierarchy of standing’ (Yar 2013). These offences were most often deemed as avoidable by officers and raised questions of personal responsibility and ownership of behaviours that may be seen as leaving a person 'open' to victimisation.

Officers engaged in negotiations with victims regarding where responsibility should lie for managing these cyber offences. They would often express their wish for the police response

to be the last point of contact for victims after contacting social media platforms, other responsible adults (like parents and schools) and personal behaviours such as deleting social media accounts and changing phone numbers. Officers engaged in boundary work whereby they were renegotiating which offences in this new remit of cybercrime they should have responsibility over, especially in an austerity climate where resources are constrained but police practice is expanding (Millie 2014). The discussion of drawing a line between included and excluded offences within the police remit anchors around considerations of the seriousness of an offence and legitimate victim status. This negotiation creates tensions not only for police officers and the conceptualisation of their own role and function but also between officers and victims.

Advising victims to ‘block’ offenders and ‘delete Facebook’ generates resistance from victims who may perceive this as victim punishment (Jane 2017a) which could result in the further exclusion of people from online spaces. It also fails to understand the centrality of online spaces in people's daily lives. Self-policing through withdrawal from online environments serves to restrict access for particular victims. This is especially problematic for victim groups who may already be experiencing forms of online othering and discrimination, for example gendered abuse aiming to silence women in online communities (Lumsden and Morgan, 2017). It may also overlook the blurring between online and offline offences such as domestic abuse, in which the withdrawal from online environments may isolate victims and further coercive and controlling behaviour (Hadley, 2017). Police officers demonstrated awareness that their advice to victims to block people or come off social media platforms was limited and often met with resistance. There was also an acknowledgement that officers needed to take online interpersonal violence seriously and direct their response at the offender. However, their responses continued to be framed in a way that suggests some

responsibility is still to be borne by the victim and officers expressed frustration at a lack of self-policing on the victim's part. This was especially the case for those offences where victim culpability was implied.

This chapter has demonstrated how officers seek to define out particular types of offences within the widening scope of cybercrime. Their attempts to 'narrow the focus' of policing (Millie, 2014) utilises perceived victim status and the seriousness of the offence as barometers of inclusion criteria. This highlights the uncertain nature of policing in relation to cybercrime as an emerging form of criminality especially within the sociocultural context of austerity. This has implication for victims of interpersonal cybercrime. The police response draws on victim blaming and victim punishment narratives which may serve to alienate victims and compound othering and discriminatory online practices. Police forces must ensure that they move beyond this approach to one which recognises the centrality of social media and online spaces in individuals' lives and seek ways to provide support for victims that acknowledges the dominance of these spaces for conducting social and political life.

References

Bossler, A. and Holt, T. (2012) 'Patrol officers' perceived role in responding to cybercrime.' *Policing: An International Journal of Police Strategies & Management* 35(1): 165-181.

Brenner, S.W. (2008) *Cyberthreats: The Emeging Fault Lines of the Nation State.* New York: Oxford University Press.

Braun, V. and Clarke, C. (2006) 'Using thematic analysis in psychology.' *Qualitative Research in Psychology* 3(2): 77-101.

Brewer, J.D. (2000) *Ethnography*. Buckingham: Open University Press.

Burns, S. and Roberts, L. (2013) 'Applying the Theory of Planned Behaviour to predicting online safety behaviour.' *Crime Prevention and Community Safety*, 15(1): 48-64.

Christie, N. (1986) 'The ideal victim.' In: E.A. Fattah (Ed.), *From Crime Policy to Victim Policy* (pp. 17-30). London: Palgrave Macmillan.

Cross, C., Parker, M. and Sansom, D. (2018) 'Media discourses surrounding "non-ideal" victims: the case of the Ashley Madison data breach.' *International Review of Victimology* ifirst doi: https://doi.org/10.1177/0269758017752410

Duggan, M. and Heap, V. (2014) *Administrating Victimization: The Politics of Anti-Social Behaviour and Hate Crime Policy*. Hampshire: Palgrave Macmillan.

Gordon, S. and Ford, R. (2006) 'On the definition and classification of cybercrime.' *Journal in Computer Virology*, 2(1): 13-20.

Greer, C. (2007) 'News media, victims and crime.' In: P. Davies, P. Francis and C. Greer (Eds.), *Victims, Crime and Society* (pp. 20-49). London: Sage.

Hadley, L. (2017) *Tackling Domestic Abuse in a Digital Age: A Recommendations Report on Online Abuse by the All-Party Parliamentary Group on Domestic Violence*. Bristol: Women's Aid Federation of England.

Her Majesty's Inspectorate of Constabulary (HMIC). (2014a) *State of Policing*. London: HMIC.

Holt, T., Bossler, A. and Seigfried-Spellar, K. (2015) *Cybercrime and Digital Forensics: An Introduction*. Oxon: Routledge.

Jagervi, L. (2014) 'Who wants to be an ideal victim? A narrative analysis of crime victims' self-presentation.' *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 15(1): 73-88.

Jane, E.A. (2017a) *Misogyny Online: A Short (and Brutish) History*. London: Sage.

Jane, E.A. (2017b) ‘Gendered cyberhate, victim-blaming, and why the internet is more like driving a car on the road than being naked in the snow.’ In: E. Martellozzo and E.A. Jane (Eds), *Cybercrime and its Victims*. Oxford: Routledge.

Laville, S. (2016) Online abuse: 'existing laws too fragmented and don’t serve victims'. *The Guardian*. URL (accessed 16 April 2018): https://www.theguardian.com/uk-news/2016/mar/04/online-abuse-existing-laws-too-fragmented-and-dont-serve-victims-says-police-chief

Lumsden, K. and Black, A. (2018) ‘Austerity policing, emotional labour and the boundaries of police work: An ethnography of a police force control room in England.’ *British Journal of Criminology*, 58(3): 606-623.

Lumsden, K. and Morgan, H.M. (2017) ‘Media framing of trolling and online abuse: silencing strategies, symbolic violence, and victim blaming.’ *Feminist Media Studies* 17(6): 926-940.

Lusthaus, J. and Varese, F. (2017) ‘Offline and local: the hidden face of cybercrime.’ *Policing: A Journal of Policy and Practice* doi: https://doi.org/10.1093/police/pax042

McAlinden, A.M. (2014) ‘Deconstructing victim and offender identities in discourses on child sexual abuse: hierarchies, blame and the good/evil dialectic.’ *The British Journal of Criminology* 54(2): 180-198.

McGarry, R. and Walklate, S. (2015) *Victims: Trauma, Testimony and Justice*. London: Routledge.

McQuade III, S.C. (2007) ‘We must educate young people about cybercrime before they start college.’ *Chronicle of Higher Education* 53(14): B29. URL (accessed April 2018): http://ra.ocls.ca/ra/login.aspx?inst=conestoga&url=http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ756806&site=eds-live&scope=site%5Cnhttp://chronicle.com/

Millie, A. (2014) ‘What are the police for? Re-thinking policing post-austerity.’ In: J.M. Brown (Ed), *The Future of Policing*. Oxford: Routledge.

Mitchell, K.J., Finkelhor, D., Jones, L.M. and Wolak, J. (2012) ‘Prevalence and characteristics of youth sexting: a national study. *Pediatrics* 129(1): 13-20.

National Crime Agency (2016) *NCA Strategic Cyber Industry Group Cyber Crime Assessment 2016*. (July), 1–16.

Navarro, J.N. and Clevenger, S. (2017) ‘Why me? Understanding cybercrime victimization.’ In: C. Roberson (Ed), *Routledge Handbook on Victims' Issues in Criminal Justice*. Oxford: Routledge.

O’Reilly, K. (2005) *Ethnographic Methods*. London: Routledge.

van Wijk, J. (2013) ‘Who is the ‘little old lady” of international crimes? Nils Christie’s concept of the ideal victim reinterpreted.’ *International Review of Victimology* 19(2): 159-179.

Wall, D.S. (ed.) (2001) *Crime and the Internet*. London: Routledge.

Wall, D.S. (2008a) ‘Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime.’ *International Review of Law, Computers & Technology* 22(1–2): 45--63.

Wall, D.S. (2008b) ‘Cybercrime and the culture of fear: social science fiction(s) and the production of knowledge about cybercrime.’ *Information, Communication & Society*, 11: 861-884.

Yar, M. (2013) ‘The policing of internet sex offences: pluralised governance versus hierarchies of standing.’ *Policing and Society* 23(4): 482-497.

Notes

[1] Study 1 was funded via a College of Policing / HEFCE Policing Knowledge Fund (Grant No. J04).

[2] *Managed Appointment Unit* – members of the public can arrange to meet a police officer within a specific time period for non-emergency matters.