Title: A qualitative enquiry into the threshold of acceptable behaviour on the internet: Perceptions of Police Officers and Prosecutors on the barriers to successful investigation and prosecution of cyberstalkers

Ori Igwe

A thesis submitted to the University of West London in fulfilment of the requirements for the degree of Doctor of Philosophy

University of West London
2 March 2020
Dedication

I dedicate this thesis to my late father Prince Chief Dr Alfred Oliwo Igwe who instilled in me that education is the foundation of success. My father passed away before I completed the thesis and shortly before he died, I had promised to make him proud by the achievement of this monumental academic goal. I wish that he were alive today to celebrate with me and witness my graduation with a Doctor of Philosophy degree.
Abstract

Cyberstalking is a cyber-enabled crime which can be difficult to investigate and prosecute because offenders engage in the conduct in cyber space. The purpose of this study is to highlight the difficulties which police officers and prosecutors perceive hinder them in the investigation and prosecution of cyberstalkers. The study identifies solutions to the perceived difficulties and makes recommendations.

The research participants consisted of 50 London prosecutors and 25 police officers. Participants provided data on the topic under investigation in their roles as the primary law enforcement officials who investigate and prosecute cyberstalkers. A Member of Parliament, probation official and Northern Ireland government policy adviser were also interviewed because they provided data from the perspectives of government and probation officials.

The qualitative research method of Interpretative Phenomenological Analysis was considered most appropriate because the study investigated the lived human experiences of the participants and their perceptions of the topic under investigation. Emergent themes were identified from the numerous interview transcripts and analysed to explore the experiences of the participants in relation to the research questions.

The research identified various perceived thresholds for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking. Additionally, the study 6 perceived law enforcement issues which frustrate police officers and prosecutors in the investigation and prosecution of cyberstalkers were identified. The
research further revealed that lack of resources, lack of knowledge and evidential difficulties are perceived to impede the investigation and prosecution of cyberstalkers. Importantly, the study found that factors such as shortage of manpower, heavy caseloads, anonymity of cyberstalkers and victim behaviour can prevent police officers from risk assessing victims.

The thesis therefore makes recommendations for the recruitment of additional staff, the regular training of police officers and prosecutors on cyberstalking and the education of victims by police officers of the risks posed by cyberstalkers and the implications of not supporting the prosecution of offenders. Importantly, the thesis recommends that police officers should be trained on how to identify, monitor and manage the risks posed by anonymous and mentally ill cyberstalkers.

The recommendation for the CPS is based on the researcher's personal view of the research. The researcher concedes that the research was conducted at a specific time and that a limited number of prosecutors were interviewed for the research. The researcher acknowledges that there has been a lot of training of prosecutors by both the prosecution college and the central training team subsequent to the conclusion of this research. The researcher also recognises that the department is in the process of actively recruiting more prosecutors.
THESIS DECLARATION

Statement 1

I hereby declare that this work has not been accepted in substance for any degree and is currently not being submitted in candidature for any degree.

Signed.................................................... (Candidate)

Date........................................................

Statement 2

This thesis is the result of my investigation, except where otherwise stated. Other sources are acknowledged by references. A bibliography is appended.

Signed.................................................... (Candidate)

Date........................................................

Statement 3
I hereby give consent for my thesis, if accepted to be available for copying and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed………………………………………………. (Candidate)

Date…………………………………………………

Statement 4

The research was completed under the guidance of:

…………………………………… (Main Supervisor) University of West London

In my capacity as main supervisor of the candidate, I certify that the above statements are true to the best of my knowledge.

Signed……………………………………………… (Main Supervisor)

Date…………………………………………………
Contents

Abstract ........................................................................................................................................... 3

Tables............................................................................................................................................. 11

Legislation ....................................................................................................................................... 12

Legislation ....................................................................................................................................... 12

Protection from Harassment Act 1997 ............................................................................................. 12

Cases ............................................................................................................................................... 12

Chapter One Introduction ........................................................................................................... 14

1.1 Jurisdictional difficulties ....................................................................................................... 18

1.2 Legislative difficulties ............................................................................................................. 21

1.2.1 Regulation of cyberstalking in the United Kingdom ......................................................... 23

1.2.2 Regulation of cyberstalking in Ireland ............................................................................. 25

1.2.3. Response of the ISPs .................................................................................................... 27

1.2.4 Evidential challenges ....................................................................................................... 30

1.2.5 Financial challenges ......................................................................................................... 35

1.2.6 Anonymity of cyberstalkers on the internet .................................................................... 36

1.3. Response of the Crown Prosecution Service (CPS) .......................................................... 40

1.3.1 Increase in prosecution of stalking cases ....................................................................... 43

1.4 Response of the Metropolitan Police Service (MPS) .......................................................... 46

1.5. Purpose of the current research ............................................................................................ 49

1.5.1. Structure of the Thesis: .............................................................................................. 53

Chapter Two Review of the literature .......................................................................................... 55

2.1 Literature Review Strategy ..................................................................................................... 55

2.2 Definition of cyberstalking .................................................................................................... 56

2.2.1 Definition of cyberstalking as an aspect of cybercrime ................................................. 59

2.2.2. The distinction between offline stalking and cyberstalking .................................... 61

2.2.3 Cyberbullying: A divergent cyber enabled crime analogous to ................................... 65
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyberstalking</td>
<td>65</td>
</tr>
<tr>
<td>2.2.4 Comparisons of Cyberstalking and Cyberbullying</td>
<td>68</td>
</tr>
<tr>
<td>2.2.5 Cyberstalking victimisation and police perceptions</td>
<td>73</td>
</tr>
<tr>
<td>2.3. Regulation of cyberstalking in England and Wales</td>
<td>79</td>
</tr>
<tr>
<td>2.3.1. An overview and critique of the Protection from Harassment Act 1997 (PHA)</td>
<td>80</td>
</tr>
<tr>
<td>2.3.2. Significance of the expanded Protection from Harassment Act 1997</td>
<td>81</td>
</tr>
<tr>
<td>2.3.3. Stalking offence under section 2A</td>
<td>82</td>
</tr>
<tr>
<td>2.3.4. Stalking offence under section 4A</td>
<td>82</td>
</tr>
<tr>
<td>2.3.5 Stalking involving a fear of violence under section 4A (1) (b) (i)</td>
<td>83</td>
</tr>
<tr>
<td>2.3.6. Stalking Involving Serious alarm or distress 4A (1) (b) (ii)</td>
<td>84</td>
</tr>
<tr>
<td>2.3.7 Legal Issues: Decision to charge and the Threshold Test</td>
<td>84</td>
</tr>
<tr>
<td>2.3.8. Legal Issues: The Full Code Test</td>
<td>86</td>
</tr>
<tr>
<td>2.3.9. The implication of legal issues under the Full Code Test and the Threshold Test on the prosecution of cyberstalkers</td>
<td>88</td>
</tr>
<tr>
<td>2.3.10. Legal issue- Meeting the Reasonable Person Test</td>
<td>89</td>
</tr>
<tr>
<td>2.3.11 Legal Issues-Defining cyberstalking implicitly and a course of conduct</td>
<td>90</td>
</tr>
<tr>
<td>2.3.12 Regulation of cyberstalking which involves hate speech crimes</td>
<td>92</td>
</tr>
<tr>
<td>2.4 Theoretical framework- Application of traditional criminological theories to cybercrime</td>
<td>97</td>
</tr>
<tr>
<td>2.4.1 Self-Control Theory: A theoretical application to cyberstalking victimisation</td>
<td>98</td>
</tr>
<tr>
<td>2.4.2 Social learning and behavioural theories of crime: Theoretical applications to cyberstalking victimisation</td>
<td>99</td>
</tr>
<tr>
<td>2.4.3 Space Transition Theory: A theoretical application to cyberstalking victimisation</td>
<td>102</td>
</tr>
<tr>
<td>2.4.4 Lifestyle Exposure Theory and Routine Activity Theory: Theoretical Frameworks Applied to cyberstalking victimisation</td>
<td>103</td>
</tr>
<tr>
<td>2.4.5 Cyberlifestyle–Routine Activities Theory: Theoretical application to cyberstalking victimisation</td>
<td>110</td>
</tr>
<tr>
<td>2.5 The UK Cybercrime Strategies</td>
<td>112</td>
</tr>
<tr>
<td>2.5.1 The Digital Britain Strategy 2009</td>
<td>113</td>
</tr>
<tr>
<td>2.5.2 The Cyber Crime Strategy and the Cyber Security Strategy: Aimed at protecting the UK in a digital world</td>
<td>113</td>
</tr>
<tr>
<td>2.5.3 The UK Digital Strategy 2017</td>
<td>116</td>
</tr>
<tr>
<td>2.5.4 National Cyber Security Strategy 2016-2021</td>
<td>117</td>
</tr>
<tr>
<td>2.5.5 National Strategic Assessment of Serious and Organised Crime for 2018</td>
<td>118</td>
</tr>
<tr>
<td>2.6 Specialist UK Cybercrime Units</td>
<td>118</td>
</tr>
<tr>
<td>2.6.1 National Crime Agency</td>
<td>119</td>
</tr>
</tbody>
</table>
## Tables

<table>
<thead>
<tr>
<th>Tables</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Experience type of police officers</td>
</tr>
<tr>
<td>Table 2</td>
<td>Experience type of prosecutors</td>
</tr>
<tr>
<td>Table 3</td>
<td>Experience type of government officials</td>
</tr>
<tr>
<td>Table 4</td>
<td>Perceptions of prosecutors on the threshold for distinguishing between rudeness, abuse and unpleasant comments on the internet and Cyberstalking</td>
</tr>
<tr>
<td>Table 5</td>
<td>Perceptions of police officers on the threshold for distinguishing between rudeness, abuse and unpleasant comments on the internet and Cyberstalking</td>
</tr>
<tr>
<td>Table 6</td>
<td>Perceptions of police officers and prosecutors on legislation</td>
</tr>
<tr>
<td>Table 7</td>
<td>Perceptions of police officers and prosecutors on the areas of lack of knowledge that frustrate them in the investigation and prosecution of cyberstalkers</td>
</tr>
<tr>
<td>Table 8</td>
<td>Perceptions of police officers and prosecutors on the areas of lack of training that frustrate them in the investigation and prosecution of cyberstalkers</td>
</tr>
<tr>
<td>Table 9</td>
<td>Perceptions of prosecutors on self-help measures that they adopt to close the knowledge gap</td>
</tr>
<tr>
<td>Table 10</td>
<td>Perceptions of police officers on self-help measures that they adopt to close the knowledge gap</td>
</tr>
<tr>
<td>Table 11</td>
<td>Perceptions of police officers and prosecutors on lack of resources</td>
</tr>
<tr>
<td>Table 12</td>
<td>Perceptions of police officers and prosecutors on risk assessment challenges</td>
</tr>
</tbody>
</table>
### Table 13
Perceptions of police officers and prosecutors on evidential challenges

### Table 14
Perceptions of police officers and prosecutors on victim behaviour

## Legislation

<table>
<thead>
<tr>
<th>Legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection from Harassment Act 1997</td>
</tr>
<tr>
<td>Protection of Freedoms Act 2012</td>
</tr>
<tr>
<td>Regulation of investigatory powers act 2000</td>
</tr>
<tr>
<td>Serious Crime Act 2007</td>
</tr>
</tbody>
</table>

## Cases

<table>
<thead>
<tr>
<th>Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>R v Blaue [1975] 1 W.L.R 1411</td>
</tr>
<tr>
<td>Chambers v DPP [2013] 1 WLR 1833 (EWCH)</td>
</tr>
<tr>
<td>R v Colohan 2001] All.ER 230</td>
</tr>
<tr>
<td>R v Qosa (Robert) 2016] EWCA Crim 1543</td>
</tr>
<tr>
<td>Lau v DPP [2000] Crim LR, 580 (QBD)</td>
</tr>
<tr>
<td>Citation</td>
</tr>
<tr>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Lord McAlpine of West Green v Bercow</td>
</tr>
<tr>
<td>Jones v DPP [2011] 1 WLR 833 (QBD)</td>
</tr>
</tbody>
</table>
Acknowledgement

Thanks to all those who participated in the research for imparting their practice knowledge and experience and for aiding me in my research work. I would like to express my heartfelt gratitude to the Crown Prosecution Service (CPS) and the Metropolitan Police Service (MPS) for consenting to the research.

I would like to express my overwhelming and heartfelt gratitude to all the individuals who have offered their support, encouragement and expertise. Thanks to my initial supervisors Professor Malcolm Davies and Dr Tony Olden for your support. I am indebted to my subsequent supervisors Professor Maddie Ohl and Dr Philipp Elliot Wright for offering their constructive criticisms and helpful suggestions. To Philip Ells, head of the School of Law at the University of West London thanks for having unwavering faith in my ability to undertake such a demanding project.

I am indebted to my late father Prince Chief Dr Alfred Oliwo Igwe and my mother Mrs Rose Ude Igwe for their never-ending encouragement. My father has taught me that hard work is the key to success. My mother has inspired me to face challenges with a smile on the face. These life lessons were a haven to me during testing moments. My son Daniel has taught me that the joys of motherhood are littered with petals of love, friendship and contentment. I would also like to thank my sister Ezinne, brothers Obi, Ebere and Iheanyi for their constant words of encouragement. Finally, I would like to thank Leroy Bunbury for being a fantastic father to our son and a gem.
Chapter One Introduction

Cyberstalking connotes the continuous targeting by repeated threats, intimidating messages, harassment, or sexual messages that are unwanted, persistent, and potentially intrusive via electronic and computer-based communication.¹ It is an emerging phenomenon of the twenty first century which poses investigative difficulties for law enforcement officials. From a legislative perspective, Basu suggests that there should be a continuous debate on the regulation of cyber space given that a unique characteristic of cyber space is that it enables behaviours to be engaged in anonymously and devoid of any geographical barriers.² Basu’s observation implicitly relates to the behaviour of cyberstalking which occurs in cyber space.

Vasiu and Vasiu contend that there could be a correlation between the commission of violent crimes and cyberstalking.³ Against this background, the fatal risk associated with cyberstalking was manifested in the death of Lorna Smith who was murdered in the UK by a cyberstalker.⁴ From an international perspective, the fatal risk associated with cyberstalking was equally highlighted in the death of Amy Boyer who was murdered by a cyberstalker in the US.⁵ Further, in Ireland, the legal advisory body of the country has highlighted that online abuse has been connected to the psychological harm suffered by victims and has also, in some cases led to victims committing

¹ Michelle Wright, ‘Cyberstalking Victimization, Depression, and Academic Performance: The Role of Perceived Social Support from Parents’ (2018) 2 CyberPsychology, Behaviour and Social Networking 2
³ Vasiu and Vasiu suggest that cyberstalking interferes with the victim’s rights to life, liberty, security and privacy. They make this observation from a human rights perspective
⁴ ‘Stalker Clifford Mills Jailed for Killing Ex-Girlfriend’ (BBC, 6 February 2012) <www.bbc.co.uk/news/uk-england-london-1613667> accessed 21 September 2017
⁵ Paul Bocjí, Mark Griffiths and Leroy McFarlane ‘Cyberstalking A New Challenge for Criminal Law’ (2002) 122 The Criminal Lawyer
suicide. These cases demonstrate that cyberstalking akin to physical stalking, can lead to the deaths of victims.

From an academic perspective, researchers have found that cyberstalking can have widespread consequences by affecting the psychological, social, interpersonal and economic aspects of life. The findings are based on recent research which has been conducted on the emotional impact of cyberstalking in the UK. The findings support the assertion of Vasiu and Vasiu that cyberstalking can have psychological, economic and physical effects on victims. From a victimisation perspective, a concern is that victims of cyberstalking who do not receive relevant support may wrongly blame themselves for being targeted by cyberstalkers. Consequently, in 2019, researchers in the UK conducted a study on how the volume and source of cyber abuse influences victim perceptions of online abuse. The study found that there was a co-relation between attractiveness and direct victim blame. The significance of this recent study is that it reveals that there is a perception that victims of cyber abuse such as cyberstalking and cyberbullying are attributed blame for the acts perpetrated against them.

An additional study which was based on 35 victims of stalking and harassment found that stalking, harassment and cyberstalking implicitly can affect victims emotionally,
psychologically and physically.\textsuperscript{11} The study found that the behaviours had an impact on every aspect of a person’s life ranging from home to work.\textsuperscript{12} The study is significant because it revealed that victims of stalking, harassment and cyberstalking implicitly include individuals who have disabilities, care for someone with a disability and/or have a substance misuse problem. Additionally, the study found that victims include individuals who have mental health issues such as depression, anxiety and physical health problems such as angina, cancer, diabetes and arthritis.\textsuperscript{13} The researcher concurs with the academics who conducted this study because victimisation of vulnerable, mentally and physically ill individuals can worsen the impact of being stalked, harassed and cyberstalked implicitly\textsuperscript{14}.

Given the severe impacts of cyberstalking on victims, the challenge for the current research was to establish the perceptions of police officers and prosecutors in London on cyberstalking and the threshold of what constitutes acceptable behaviour on the internet. In doing so, the researcher examined the issues of the risk assessment of victims and the factors which frustrate the attempts of both police officers and prosecutors in the investigation and prosecution of cyberstalkers.

The researcher interviewed 63 UK law enforcement officials comprising of 25 police officers, 30 prosecutors, 1 probation officer, 1 Member of Parliament and 1 Northern Ireland government adviser.

\textsuperscript{11} ‘The Victim’s Journey participatory research project seeking the views and experiences of victims of stalking and harassment’ (Justice inspectorate, July 2017) <A participatory research project seeking the views and experiences of victims of stalking and harassment> accessed 6 May 2019

\textsuperscript{12} Out of the 35 participants, 14 completed an online survey, 5 were interviewed face to face and 16 were interviewed over the telephone

\textsuperscript{13} ‘The Victim’s Journey participatory research project seeking the views and experiences of victims of stalking and harassment’ (Justice inspectorate, July 2017) <A participatory research project seeking the views and experiences of victims of stalking and harassment> accessed 6 May 2019

\textsuperscript{14} The implicit cyberstalking behaviours experienced by the participants include stalking via social media, phone calls, text messages and recording/taking pictures with a mobile phone
The factors listed below have been identified as posing a potential hindrance to the investigation of cyberstalkers.

1.1 Jurisdictional difficulties

Jurisdictional difficulties constitute an obstacle for law enforcement officials because the unlimited reach of the internet enables cyberstalkers to harass victims instantaneously, cheaply and globally even when the cyberstalkers and the victims are in different geographical locations. From the perspective of victims, it has therefore been acknowledged that the fact that cyberstalkers can contact the victims from any jurisdiction can lead to victims living in a state of fear, terror, stress, anxiety or intimidation.

From a geographical perspective, there are two jurisdictional dimensions to Cyberstalking which could determine the extent to which international cooperation is required to bring a cyberstalker to justice. The first jurisdictional dimension entails cyberstalking which occurs when the cyberstalker and the victim reside in the same country. The second jurisdictional dimension encompasses cyberstalking which occurs cross-jurisdictionally where the cyberstalker and the victim reside in different countries.

---

From a law enforcement perspective, the first dimension to cyberstalking may pose little or no jurisdictional difficulties given that the victim and the perpetrator reside in the same geographical location. The second jurisdictional dimension on the other hand is more problematic for UK law enforcement officials given that there will be an onus on the other countries to cooperate with UK police officers and prosecutors during the investigation process. The second dimension is problematic because it is questionable whether the law enforcement officials in the other countries will cooperate with the UK police officers during the investigation process.

From a jurisdictional perspective, prior to investigating a case, UK police officers will have to establish that an offence has been committed and ascertain which criminal law will be applicable. Against this background in relation to the investigation of cybercrime, Brown highlights that several factors such as ascertaining where a crime was committed and dealing with conflicting laws can create problems for police officers, prosecutors and judges. Brown argues that the difficulties can make it challenging to issue warrants, draft subpoenas and conduct trials.

From an extradition perspective, when investigating a case where a cyberstalker and the victim reside in different jurisdictions, UK police officers and prosecutors face the related difficulty of identifying which jurisdictional law will be applicable to a given case. This is because the law enforcement authorities in a cyberstalker’s country of residence could refuse to extradite a suspect on the grounds that they do not extradite nationals. Consequently, Shearer argues that some international extradition treaties

---

18 Applying Brown’s line of reasoning to the conduct of cyberstalking which is an aspect of cybercrime, UK police officers and prosecutors may encounter similar difficulties in the investigation of cyberstalkers given the jurisdictional and legislative implications of prosecuting cyberstalkers
may contain either mandatory or discretionary bars to the extradition of nationals exempting countries from extraditing citizens. Shearer suggests that there is no moral duty on countries to extradite a fugitive in the absence of an extradition treaty.

Another aspect of the jurisdictional problem is that sometimes, cyberstalkers perpetrate the offence from several jurisdictions when the victim and the cyberstalker reside in different countries. Therefore, Ogilvie stresses that confirmation has to be sought regarding which jurisdiction has the responsibility of regulating cyberstalking where for example, a suspect harasses a victim from four different jurisdictions.

Ogilvie notes that the borderless feature of cyberstalking and challenges of legislative control make it difficult to establish which jurisdiction has the responsibility prosecuting a cross-jurisdictional cyberstalker.

Against the above background, previously conducted research has indicated that the investigation of cyberstalkers can be hindered by certain difficulties. In particular, a study was conducted on the number of cases that were handled by the New York Police Department’s Computer and Investigation unit. The study examined the number of cases that were handled by the New York City department between January 1996 and 2000 involving the use of the computer or the internet by criminals to perpetrate the offence of aggravated harassment which is synonymous to

19 Ivan Shearer, ‘Non-Extradition of Nationals: A Review and a Proposal’ (1966) 2 Adelaide Law Review Association 3
20 Applying Shearer’s line of reasoning to the study, it is debatable whether foreign countries will honour the requests of UK police officers to extradite cyberstalkers if there are no extradition treaties. This area of uncertainty therefore casts a doubt on the effectiveness of extradition as a law enforcement method of international cooperation in this regard
21 The ability of cyberstalkers to perpetrate the offence from various geographical locations could undermine the efforts of UK police officers to seek the prompt extradition of suspects
22 Emma Ogilvie, ‘Cyberstalking Trends and Issues in Crime and Criminal Justice’ (2005) 166 Australian Institute of Criminology
23 It is therefore questionable whether police officers in the UK can successfully investigate a cross-jurisdictional cyberstalker where the perpetrator sends offensive and threatening messages to a victim resident in the UK for example and then flees to Ireland and subsequently, the US from where he sends further messages
cyberstalking. 25 The study found that 192 out of 201 cyberstalking cases were closed without any action having been taken against the perpetrators even after evidence was found to support a victim’s allegation.

In summary, UK police officers will encounter jurisdictional difficulties in seeking to prosecute cyberstalkers given that there are no geographical barriers to the behaviour. Considering the above observations, it is arguable that UK police officers may successfully prosecute cyberstalkers who are resident in other countries subject to the jurisdictional challenges identified above being overcome, however the focus of this thesis is the investigation and prosecution of cyberstalkers in the UK.

1.2 Legislative difficulties

There is generally no accepted definition of cyberstalking. 26 This lack of a universal definition has arguably placed an onus on countries including the UK to enact adequate legislation regulating the criminal behaviour of cyberstalking. Consequently, Van der Aa notes that as is the case with traditional stalking, it is a challenge to define cyberstalking. 27 Van der Aa highlights that an aggravating factor is deciphering whether cyberstalking should be viewed as a new type of criminal behaviour or simply an aspect of stalking in the physical realm. 28

25 The significance of the research findings is twofold. First, it established that jurisdictional difficulties could hinder the investigation of cyberstalking cases. Second, the research highlighted that the police could be reluctant to investigate such cases if cyberstalkers and victims reside in different locations.


27 Suzanne Van der Aa, ‘International (Cyber) stalking, Impediments to Investigation and Prosecution’ (Pure, 1 January 2011)

28 This area of uncertainty can create legislative difficulties insofar as it results in countries either adopting different legislative approaches to criminalising cyberstalking in the absence of a universally accepted definition for the behaviour or choosing not to regulate the conduct.
Given that cyberstalking needs to be a proscribed conduct for perpetrators to be brought to justice, relevant legislation needs to be enacted to criminalize and regulate the conduct. This is more so because the legal system is not structured to tackle offences committed by cybercriminals in the cyberworld.\textsuperscript{29} Basu implies that there is a perception that legislation will only be an effective means of control if the cyberstalker can be identified. Against this backdrop, Geach and Haralambous suggests that to ensure that the law is definite, the legislation should provide a clear and precise definition of cyberstalking.\textsuperscript{30} Geach and Haralambous emphasise that in the information and technology sector, criminalising a conduct that is specific to online acts may be problematic if due to technological advancement, a particular technology becomes so outdated that it no longer matches the technology as specified in an offence.\textsuperscript{31}

Two aspects of legislative difficulties could hinder the efforts of UK police officers and prosecutors to prosecute cyberstalkers. The first aspect is that existing legislation may not specifically prohibit cyberstalking thereby placing an onus on UK police officers to establish that an offence has been committed. The second aspect of the legislative difficulty is that perpetrators could threaten victims from countries where no laws on cyberstalking exist. In the jurisdiction of Ireland for example, no legislation has been enacted to criminalize either offline stalking or cyberstalking. Consequently, O'Keeffe, highlights that the law reform commission in Ireland has recommended the creation of

\textsuperscript{29} Subhajit Basu and Richard Jones, ‘Regulating Cyberstalking’ (2007) 2 Journal of Information Law and Technology
\textsuperscript{30} Neal Geach and Nicola Haralambous, ‘Regulating Online Harassment: Is the Law fit for the Social Networking Age?’ (2009) 73 Journal of Criminal Law 3
\textsuperscript{31} Geach and Haralambous highlight that in such situations, the technology develops into something which no longer matches, what is defined in the offence
new offences to tackle online abuse in respect of cyberbullying and revenge pornography.\textsuperscript{32}

In consideration of the above, this research will focus on the investigation and prosecution of cyberstalking in the UK as a specific cyber enabled aspect of cybercrime.

\subsection*{1.2.1 Regulation of cyberstalking in the United Kingdom}

In the UK following public concern, the coalition government attempted to regulate cyberstalking on 25 November 2012 via the amendment of the Protection from Harassment Act (PHA).\textsuperscript{33} The PHA was consequently expanded via sections 2A (1), 4A (i) (b) (i)) and 4A (i) (b) (ii) respectively to create the statutory offences of “stalking”, “stalking involving fear of violence” and “stalking involving serious alarm or distress”.

From a law enforcement perspective, although cyberstalking is not specifically defined as an offence, the newly created laws have been drafted broadly to incorporate elements of cyberstalking.\textsuperscript{34} The researcher therefore anticipates that the legislative amendments will assist UK police officers and prosecutors to an extent in the investigation and prosecution of cyberstalkers.

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{32} Cormac O’Keeffe, ‘New Laws to Combat Online Abuse such as Cyber Bullying and Revenge Porn’ (Irish Examiner, 27 September 2016) <www.irishexaminer.com/ireland/new-laws-to-combat-online-abuse-such-as-cyber-bullying-and-revenge-porn-422963.html> accessed 9 August 2018
\item\textsuperscript{33} Section 111 of the Protection of Freedoms Act 2012 came into force on 25 November 2012 thereby creating the new offences of stalking and stalking involving serious alarm or distress
\item\textsuperscript{34} Section 2A (3) of the Protection from Harassment Act 1997 gives seven examples of acts or omission which amount to stalking. Five of the examples under ss 2A (3) (b) (c) (d) (f) and (g) highlight activities carried out by cyberstalkers
\end{itemize}
\end{footnotesize}
In Northern Ireland which is part of the UK, there is no specific legislation on stalking and cyberstalking. This has led to the committee of justice embarking on a review of the need to for stalking legislation in Northern Ireland. To this effect, in making a submission to the committee, academics at the Queen’s University of Belfast, School of Law, concluded that the current law in Northern Ireland is not effectively tackling stalking.\(^{35}\) The academics suggested that a specific legislation on stalking would ensure that stalking is effectively tackled. This implies that it is vital for legislation on cyberstalking to be enacted with a view to regulating the behaviour and holding perpetrators accountable for their actions.\(^{36}\) Against this backdrop, Holt, Bossler and Seigfried-Spellar highlight that certain factors such as the cheap prices of technological gadgets, the easy access of technology, the minimal technical knowledge required to commit some offences and the ability to instantaneously victimise on a large scale globally, collectively make cybercrime and cyberdeviance attractive to offenders.\(^{37}\) Holt, Bossler and Seigfried-Spellar’s observations implicitly relate to cyberstalkers who as cyberdeviants, are a specific breed of cybercriminals.\(^{38}\)

In summary, it can therefore be argued that the legislative measures which have been taken by the UK parliament in 2012 to create the 2 new offences of stalking and stalking involving serious alarm or distress, is a step in the right direction given that police officers and prosecutors in the UK can utilise the legislation as a tool to bring cyberstalkers to justice. Further from a civil law perspective, the recently enacted Stalking Protection Act 2019 has provided police officers with an additional tool to


\(^{36}\) This is more so because if cybercrime is not regulated via legislation, it could lead to perpetrators avoiding extradition and prosecution due to lack of legislation

\(^{37}\) Thomas Holt, Adam Bossler and Kathryn Seigfried-Spellar, Cybercrime and Digital Forensics (2nd edn, Routledge 2018) 1

\(^{38}\) Holt, Bossler and Siegfried-Spellar point out that the risk of detection from law enforcement is lower in the cyber realm than in the physical realm
The Stalking Protection Act 2019 creates a new civil stalking protection order to protect members of the public from risks associated with stalking and empowers police officers to make applications for a new order to a magistrates’ court. Therefore the Home Office explanatory note emphasises that the intention of the Act is to provide the police with an extra weapon with which to protect victims of stalking and to fill a gap within the existing protective system. The significance of the new stalking order is that it enables Police officers to utilize the order as a tool for protecting victims in five different cases as discussed in the Home Office explanatory note.

1.2.2 Regulation of cyberstalking in Ireland

In comparison to the UK government, Ireland has not taken legislative steps to criminalize cyberstalking. Hence, Gleeson highlights that there is a call for cyberstalking laws to be updated. McCarthy echoes Gleeson’s view and emphasises that to regulate cyberstalking in Ireland, the current legislation banning harassment and threats will be extended to criminalize online activity and social media activities especially.

The implication is that Irish law enforcement officials still utilise existing legislation on harassment to prosecute perpetrators in the absence of a specific cyberstalking

41 ibid
42 The cases are when the does not occur in a domestic abuse situation, context, or offenders are strangers who are not the current or previous partners of victims; the criminal threshold has not, or has not yet, been met or the victim does not support a prosecution
44 Kieran McCarty ‘Ireland to make Revenge porn, Cyberstalking Criminal Acts’ (Register, 16 May 2017) <https://www.theregister.co.uk/2017/05/16/ireland_cyberstalking_criminal/> accessed 18 December 2019
The inadequate legislative situation in Ireland highlights the second of the legislative difficulties identified above which is that some countries are yet to criminalize cyberstalking.

The fact that cyberstalking is yet to be criminalised in Ireland has led to public concern among certain sectors in Ireland. Consequently, on 12 February 2014, the Women’s Aid Domestic Violence charity in Ireland launched an awareness campaign requesting a legislative change to tackle digitally assisted stalking or cyberstalking. The outcome of the campaign was that there was a heightened public awareness on the effects of cyberstalking on victims in so far as it relates to domestic violence. Further, the independent Law Reform Commission in Ireland conducted a public consultation on whether the harassment offence in section 10 of the Non-Fatal Offences against the Person Act 1997 should be amended to incorporate a specific reference to cyber harassment. Baker notes that in seeking legal opinion on whether a specific legislation was required for cyber harassment, the Irish Law Reform Commission requested that members of the public comment on issues such as the creation of harmful websites and fake profile pages on social networking sites in order to impersonate the victim and post harmful or private messages in the victim’s name.

On 6 October 2014, the findings of the Law Reform Commission in Ireland were published. The commission recommended among other things that a specific reference to cyber harassment in section 10 of the Non-Fatal Offences against the

---

45 The primary legislation is section 10 of the Non-Fatal offences against the Persons Act 1997. The statute creates the offence of harassment and prohibits the harassment of a person by any means without lawful authority or reasonable excuse.

46 ‘Women’s Aid Urges Government Action on Stalking and Abuse Among Young Women’ (Women’s Aid, 13 February 2014) <www.womensaid.ie/newsevents> accessed 17 April 2016

47 Jennifer Baker, ‘Ladies and Trolls: Should We Make Cyber bullying a Crime?’ (The register, 5 January 2015) <www.theregister.co.uk/2015/01/05/speak_your_brains_should_we_criminalise_cyber_bullys_asks_ireland/> accessed 9 August 2018
Person Act 1997 should be incorporated into the legislation as it would clarify the scope of the section and might increase the reporting and the prosecution of cyber harassment cases.\textsuperscript{48} The researcher anticipates that if the recommendation is implemented, the UK police officers investigating a cyberstalker in Ireland could argue that the amended legislation which expressly prohibits cyber harassment via any means, implicitly prohibits cyberstalking too.

The Law Reform Commission in Ireland has also recommended the creation of new offences to tackle online abuse in respect of cyberbullying and revenge pornography.\textsuperscript{49} Notably, Bardon highlights that the Irish government will draft the Non-Fatal Offences (Amendment) Bill to address loopholes in current legislation in order to criminalize stalking, including cyberstalking, and revenge porn criminal offences.\textsuperscript{50} It is anticipated that the legislative change will extend the offence of harassment to ensure it includes activity online and on social media.

1.2.3. Response of the ISPs

Given the global and technologically reliant features of cyberstalking, there is a public expectation that the internet companies such as Google and Facebook should have responsibility to introduce specific measures to tackle the use of the internet to disseminate offensive messages in addition to addressing online harassment in


\textsuperscript{49} Cormac O’Keeffe, ‘New Laws to Combat Online Abuse such As Cyber Bullying and Revenge Porn’ (Irish Examiner, 27 September 2016) \<www.irishexaminer.com/ireland/new-laws-to-combat-online-abuse-such-as-cyber-bullying-and-revenge-porn-422963.html> accessed 9 August 2018

general and cyberstalking specifically. Such public expectation is understandable given that cybercriminals are utilising the internet to commit further offences in addition to cyberstalking. To this effect, on 18 January 2018, Wilkinson and Kelly reported that drug dealers are using Facebook, Instagram and Twitter as platforms to sell drugs to children on social media websites.51

From a law enforcement perspective on 7 February 2017, it was further reported that Twitter had announced new measures to tackle abuse and online harassment.52 It was envisaged that the highlighted measures would protect customers from abuse and harassment, stop banned users from creating new accounts and introduce a feature which will enable the company to remove sensitive tweets.53 Specifically, it was highlighted that Twitter had previously banned prominent individuals for either engaging in or instigating the targeted abuse of individuals and had additionally suspended the accounts of 360,000 customers for violating its policies against the promotion of terrorism and violent extremism.

In addition to the above, Wilkinson and Kelly emphasise that Facebook employed an extra three thousand people to review the videos of crimes and suicides in light of murders that have been broadcasted live on the network.54 Further, it has been stressed that Google has recently introduced a new measure to identify and remove offensive materials on YouTube.55 The observation was made from two standpoints.

51 Ben Wilkinson and Tom Kelly ‘The Facebook Drug Dealers Exposed: Cannabis Peddled to Children on Social Media’ Daily Mail (London, 18 January 2018) 1
53 ibid
54 ‘Facebook to Hire Another 3,000 People to Review Videos of Crime and Suicides’ (Belfast Telegraph, 3 May 2017) <www.belfasttelegraph.co.uk/business/technology/facebook> accessed 17 January 2018
55 ‘Google Bows to Pressure to Tackle Extremists’ (The Week, June 20 2017) <www.week.co.uk/85809-google-bows-to-pressure-to> accessed 19 January 2018
The first standpoint suggests that Google will recruit independent experts to assist the company while adopting a strict approach to the removal of videos that violate the policies of the company. The second standpoint demonstrates that Google will expand the role of YouTube in combating the radicalization of individuals online by terrorists.

It is evident from this that Twitter, Facebook and Google respectively are taking some measures to tackle the dissemination of offensive messages via the internet albeit without making specific reference to cyberstalking as an aspect of cybercrime. However, in light of the current international political climate and the constant global threat of terrorist attacks, the researcher is of the view that there may be a danger of the government and the ISPs focusing principally on the constant threat of cyber terrorist attacks and the related problem of the radicalization of individuals on the internet by extremists as opposed to the activities of cyberstalkers.

Against the above backdrop, MacAskill highlights that Ciaran Martin the head of the National Cybersecurity Centre has warned that a major cyber-attack in the UK which could disrupt British elections and infrastructures is inevitable. The observation was made from a perspective which suggests that such an attack is anticipated to happen in the next two years and measures have to be implemented to address the threat. The implication is that cyberstalking may not be considered a priority for the UK government in comparison to certain topical cybercrimes.

56 The measures range from the removal of offensive materials on the internet to suspending the accounts of cybercriminals
57 The researcher recognizes that in light of the regular media reporting of terrorist attacks and the radicalization of youths, there is a danger of the government and the ISPs justifying their envisaged decision to focus primarily on cyber security on the grounds that cyber terrorists and extremists pose a real and serious threat to national security
Despite the various measures discussed above which have been implemented by Twitter, Facebook and Google on 17 January 2020, a report prepared by the Royal College of Psychiatrists on technology and the mental health of children and young people was published which identified several measures that social medial companies and ISPs arguably should implement to protect children and young people. The measures are for social media companies to highlight communication with risky content, offer assistance to vulnerable people, liaise with mental health charities and fund media literacy awareness campaigns. The report is crucial because it demonstrates that the debate on the onus of the social media companies and ISPs to protect victims is ongoing.

### 1.2.4 Evidential challenges

The ability of UK police officers and prosecutors to gather incriminating electronic evidence is a pre-requisite for the successful prosecution of cyberstalkers. Without the required evidence, Prosecutors will be unable to build strong cases against perpetrators. This is more so because, as the primary prosecuting authority in the UK, the Crown Prosecution Service (CPS) is required to apply the full code test which is set in the CPS code for crown prosecutors. The test comprises of the evidential and the public interest tests.

---


60 ibid

61 The Incriminating evidence will be crucial for the prosecution of cross-jurisdictional cyberstalkers

62 The electronic evidence includes emails, phone data and electronic printouts from the various social networking sites such as Twitter and Facebook

Based on the Evidential Test, UK prosecutors will have to decide whether the evidence presented is sufficient and credible to charge a cyberstalker and whether there is a realistic prospect of convicting them. Additionally, if there is sufficient evidence to warrant a prosecution or settlement out of court, prosecutors will also be required to apply the public interest test to decide whether it is in the public interest to prosecute a cyberstalker.64

The significance of the public interest questions is that the questions which are not exhaustive, enable prosecutors to ascertain the relevant public interest factors tending for and against prosecution. Crucially, the public interest test requires prosecutors to consider seven questions. The first, second and third questions consider the seriousness of the offence, the level of culpability and the circumstances of and the harm caused to the victim. The fourth, and fifth public interest questions to be considered by prosecutors are the suspect’s age and maturity at the time of the offence and the impact on the community. The sixth and seventh questions require prosecutors to consider if prosecution is an appropriate response and if sources of information require protecting.65

There is an onus on UK police officers to ensure that during the investigation of cyberstalkers, the electronic evidence is retrieved legally, stored appropriately and analysed by a computer forensic expert if required. This is more so given that the electronic evidence could be lost or rendered inadmissible in court if they are not preserved properly or obtained after following proper procedures.66

64 ibid
65 ibid
From a legal perspective, if police officers believe that a cyberstalker has committed an indictable offence and that evidence of that offence is in the cyberstalker’s premises, they will be legally required to obtain a search warrant. The significance of the warrant is that it may also authorize persons accompanying the police officers conducting the search such as computer experts. Consequently, there is an onus on UK police officers to ensure that they obtain search warrants and comply with applicable jurisdictional legislation prior to searching, confiscating and storing the computer devices of perpetrators. Where the onus is not discharged, there is a risk that any evidence obtained from such searches will be rendered inadmissible at trial. The difficulty for UK police officers is ensuring that they adhere to jurisdictional laws when investigating cyberstalkers given that the laws may be divergent.

Marion highlights that it is not always easy to obtain and preserve the evidence required to prove a cyberstalker’s criminal identity or to acquire and preserve electronic evidence. Therefore, Burmester, Henry and Kermes emphasise that digital evidence presents a new challenge for law enforcement officials seeking to prosecute cyberstalkers due to its easily corruptible features. Burmester, Henry and Kermes have further argued that accessing the digital evidence stored in foreign jurisdictions could significantly complicate the investigation process, more especially where an offender resides in a given country and the required digital evidence is in a different country.

69 ibid
Cyberstalking contains a lot of digital evidence given that cyberstalkers tend to leave a trail of digital evidence when disseminating malicious messages.\textsuperscript{71} From an evidential perspective, UK police officers will be required to send a preservation order to an ISP in a bid to prevent any change or deletion of a cyberstalker’s data until a court order or a search warrant has been obtained. Sammon argues that a preservation order will prevent an ISP from deleting existing data pertaining to an internet subscriber, which indirectly includes a cyberstalker.\textsuperscript{72} There is therefore an obligation on UK police officers and prosecutors to obtain, secure and preserve the required digital evidence to enable them to build robust cases against cyberstalkers.\textsuperscript{73}

On obtaining a preservation order, UK police officers are expected to submit the search warrant, court order or subpoena to the social media provider and the ISP with a view to obtaining the relevant data. The preservation order must be in relation to a specific account and time frame.\textsuperscript{74} The researcher however envisages that the criteria might create evidential difficulties where the identity of the cyberstalker is anonymous. In such a scenario, an ISP may be unable to store and save the existing data that is specific to an anonymous cyberstalker.\textsuperscript{75}

A further dimension to the evidential challenge faced by UK law enforcement officials is that where electronic data is publicly accessible on the internet, there is an onus on UK police officers to ensure that subsequent investigations do not infringe on a

\textsuperscript{71} The digital evidence consists of internet history records, emails, instant messaging, blogs, text messages and videos among others
\textsuperscript{72} John Sammon, (2015), Digital Forensics: Threatscapes and Best Practice (first published, 2015) 62
\textsuperscript{73} To fulfil this obligation, UK police officers will be required to overcome the evidential hurdle of obtaining a judicial warrant to either seize the digital evidence or to request for it to be produced
\textsuperscript{74} John Sammon, (2015), Digital Forensics: Threatscapes and Best Practice (first published, 2015) 62
\textsuperscript{75} This is because, in theory, prior to obtaining a search warrant or production order, UK police officers are required to obtain a preservation order for the retention of a cyberstalker’s computer data. In reality however, it might be a challenge for the UK police officers to obtain the preservation order if a cyberstalker is anonymous
cyberstalker’s right to privacy which is guaranteed under Article 8 of the European Convention of Human Rights 1953. The right governs the processing of data relating to the private lives of individuals which implicitly includes the likes of cyberstalkers and other criminal deviants.\textsuperscript{76} Given that cyberstalkers can argue that they have a reasonable expectation of privacy in relation to the information stored on their electronic devices which should not be subject to police investigations, there is a further onus on UK police officers to ensure that there is a legal basis for obtaining publicly accessible data on the internet which pertains to a cyberstalker.\textsuperscript{77}

In addition to the above, a further evidential difficulty which could be encountered by UK police officers is that it may be difficult for them to establish the computer that was used by a cyberstalker to disseminate offensive messages or to prove the identity of the perpetrator. This is because, the relevant computer may be in a public library or an internet cafe.\textsuperscript{78} Geach and Haralambous therefore argue that there is no guarantee that the identification of a computer which was used by a cyberstalker to perpetrate a cyberstalking act will provide an evidential link to the cyberstalker.

In summary, UK police officers and prosecutors will face various evidential and procedural issues in seeking to obtain, preserve and analyse the digital evidence required to prosecute cyberstalkers. The challenge for UK police officers and prosecutors is to overcome the highlighted difficulties with a view to building robust cases against cyberstalkers and bringing them to justice.

\textsuperscript{77} ibid
\textsuperscript{78} Neal Geach and Nicola Haralambous, ‘Regulating Harassment: Is the Law Fit for the Social Networking Age?’ (2009) 72 Journal of Criminal Law 31
1.2.5 Financial challenges

The prosecution of cyberstalkers will involve the analysis of electronic intangible evidence. Consequently, the investigating police officers may be required to instruct forensic experts in an attempt to recover and analyse electronic data from the electronic gadgets of cyberstalkers. The forensic experts play a significant role in the investigation process because they assist in the analysis of coded materials which could connect a cybercriminal to an offence. To this effect, Casey suggests that encryption can constitute a strong obstacle in the forensic examination of digital evidence. Casey highlights that the computer forensic examiners will assist in the recovery of encrypted data which have been used by criminals to conceal incriminating evidence.

The difficulty for UK police officers is establishing that it is justifiable to instruct forensic experts who will be tasked with analysing, recovering and interpreting encrypted digital data which have been used by cyberstalkers to conceal incriminating evidence given the financial implications. A further financial difficulty which UK police officers could encounter is establishing who will pay the fees of the forensic computer expert. The Metropolitan Police Service acknowledges that the process of obtaining computer evidence could be expensive but nevertheless, contends that if handled effectively, it could provide compelling evidence. It is however, questionable whether

---

79 In doing so, the police officers will face the financial challenge of instructing computer forensic experts thereby incurring expenses.
81 ibid
cyberstalking would be prioritised as a serious offence justifying the very high costs that will be incurred in obtaining crucial computer evidence.\textsuperscript{83}

In addition to the above, financial expenses will be incurred when the UK law enforcement officials commence extradition proceedings against a cyberstalker. In effect, the extradition of a cyberstalker will involve public funding. Crucially, critics may argue that it is not justifiable for police officers to spend significant amounts of public funds on the extradition of cyberstalkers if the public view is that the cyberstalkers probably do not pose the same level of threats to society in comparison to other criminals such as murders, rapists, paedophiles and terrorists. However, given that some perpetrators have ended up killing victims, it could be counter argued that it is in the interest of both the victims and society for cyberstalkers to be brought to justice by extraditing, prosecuting and sentencing them accordingly.\textsuperscript{84}

\subsection*{1.2.6 Anonymity of cyberstalkers on the internet}

Anonymity connotes the ability of individuals to utilise the internet without disclosing personal information that might enable other internet users to identify them.\textsuperscript{85} The internet affords cyberstalkers the opportunity to harass, intimidate and threaten victims under the cloak of anonymity. Against this backdrop, Roberts highlights the anonymity of the internet as an investigative problem for law enforcement officials given that the perpetrators, within it, can hide their identities by sending forged and anonymous

\textsuperscript{83} Whether cyberstalking is classified as a serious offending behaviour justifying exorbitant law enforcement expenditure is contingent on cultural trends and the perceptions of recipients

\textsuperscript{84} From a domestic perspective as previously mentioned, this is evident in the case of Lorna Smith who was murdered by a cyberstalker in the UK. From an international perspective, the fact that cyberstalking can result in the death of a victim was equally highlighted in the case

\textsuperscript{85} Yair Amichai-Hamburger ‘The Social Net understanding Our Online Behaviour’ (2\textsuperscript{nd} edn, OUP 2013)
communications. Roberts argues that cyberstalkers are able to communicate in cyberspace without revealing their identities by utilising anonymous re-mailing services. Marion therefore suggests that law enforcement officials have been unable to respond effectively to the threats which are posed by individuals who utilise computers to commit crimes.

The problem of cyberstalkers being anonymous has been compounded by the fact that certain business establishments offer services which enable customers to communicate anonymously. In particular, such organisations have developed technological devices which are used by customers to threaten individuals and public organisations in the cyber-world. Against this background, Patrick highlights that by using the anonymous re-emailer service, a cyberstalker can interact with a victim via email without the cyberstalker revealing his true identity. Patrick emphasises that a re-emailer, removes the original header of an email and then forwards the message on to a victim with a new email header. Further, Harvey suggests that the re-emailer service provides anonymity by removing all identifying information from an email and attaching a random replacement header. In light of Patrick and Harvey’s observations, the implications for UK law enforcement officials is that where cyberstalkers use the anonymous messaging apps to disseminate communications, they can potentially evade detection, arrest, prosecution and punishment.

---

88 Ibid
90 In doing so, a cyberstalker is able to conceal his identity more especially, when he uses a re-mailer which does not give the victim an option to reply to messages
91 David Harvey, ‘Cyberstalking and Internet Harassment: What the Law Can Do’ (Victims of crime, 1 January 2003) <www.victimsofcrime.org/docs/Information%20Clearinghouse/Cyberstalking%20and%20Internet%20Harassment%20What%20the%20Law%20can%20do.pdf> accessed 11 August 2018
Another dimension of the investigative hurdle is that anonymous cyberstalkers make things more difficult by either utilising technological encryption techniques or assuming the identity of another person. In doing so, they can hinder the investigation process by disseminating messages to victims via computers in more than one country which are inaccessible to law enforcement officials.\textsuperscript{92}

If the identity of an alleged cyberstalker is known and the offensive messages have been traced to the internet portal address of a suspect, there will be a further onus on UK prosecutors to prove that the offensive messages were personally disseminated by the suspect. As previously highlighted, this might be problematic where a computer is located in a publicly accessible area given that the cyberstalker may argue that a third party accessed his computer to send the messages.\textsuperscript{93}

From a legal perspective the anonymity of cyberstalkers could make it difficult for prosecutors to satisfy the Evidential Test of establishing that there is a realistic prospect of conviction due to the fact that a robust case cannot be built against an anonymous cyberstalker whose real identity cannot be established.\textsuperscript{94} The anonymity of cyberstalkers may also prevent UK police officers from being able to obtain an arrest warrant or to seek the extradition of an unidentified cyberstalker.

\textsuperscript{92} For the purposes of this research study, the investigative problem can arise for UK law enforcement officials where cyberstalkers resident in Ireland or the US for example, utilize encryption techniques, different ISP addresses or fake online screen names to hide their identities when communicating with victims in the UK.

\textsuperscript{93} This scenario may arise where a cyberstalker is sharing his accommodation with other tenants or where the relevant computer is located in a public library, community centre, or internet shop.

\textsuperscript{94} Crown prosecutors are required to apply the full code test which comprises of evidential and public interest tests prior to charging a suspect.
To avoid cyberstalkers escaping justice, UK law enforcement officials can attempt to unmask the identity of a cyberstalker by liaising with the relevant ISPs with a view to obtaining the internet portal addresses of suspects and tracing the origins of the offensive email correspondence.95

Given that Google, Yahoo and Facebook all have their headquarters in the US, there is a procedural requirement for UK police officers to obtain a court order for information about cyberstalkers to be disclosed in the country of the headquarters. To this effect, Goodno highlights that the US Federal Cable Communications Policy Act of 1984, stipulates that the records of a subscriber will not be disclosed to law enforcement officials without a court order.96 Goodno therefore argues that the protection of an internet subscriber’s details by the ISPs can constitute a barrier to combating cyberstalking.

In addition to the above, the ISPs may be reluctant to disclose the data held on cyberstalkers without their prior consent to avoid potential breaches of privacy arguments. Suffice it to say that the evidential data may be inaccessible to UK police officers if the ISPs refuse to provide the communication data of customers for privacy reasons.

In summary, the collective investigative difficulties identified above coupled with the fact that ISPs may be reluctant to provide the evidence required to prosecute

---

95 The internet portal address is a unique address which is given to each customer who subscribes to services rendered by the ISPs. The internet portal address is significant because it can establish the origin of an email correspondence and identify the actual email account from which the message has been disseminated

cyberstalkers demonstrates that UK police officers face a daunting task in the prosecution of cyberstalkers. Suffice it to say that factors such as the anonymity on the internet, jurisdictional limitations, statutory limitations, evidential limitations and resource limitations are five investigative impediments which can hinder the efforts of UK police officers and prosecutors to bring cyberstalkers to justice.

1.3. Response of the Crown Prosecution Service (CPS)

The Crown Prosecution Service (CPS) is a government department which is completely independent of the police and prosecute criminals in England and Wales. In advising the police on possible prosecutions, the CPS carries out various functions ranging from applying the CPS code for crown prosecutors when reviewing cases to preparing the cases for trial. When arriving at decisions on whether or not to charge a suspect or proceed with a prosecution, the CPS applies the Threshold Test which consists of two stages. The tests are discussed in detail in Chapter 2 (Sub-section 2.3.8).

As the primary organisation, responsible for prosecuting criminal cases in the UK, the CPS has implemented measures to assist prosecutors reviewing cyberstalking cases. To this effect on 29 September 2010 the CPS published revised guidance for prosecutors on stalking.

---

98 ibid
Given that the emerging criminal behaviour of cyberstalking has led to legislative changes in the UK (comprehensively discussed in Chapter 2 section 2.3), the CPS has taken steps to enlighten prosecutors and members of staff on the relevant changes. Specifically, on 22 January 2013, the CPS notified staff members via the internal communications gateway system that the organisation had amended the legal guidance on the Protection from Harassment Act 1997 (PHA) to incorporate the new offences of stalking and stalking involving fear of violence or serious alarm or distress. The offences were created under the newly inserted s2A and s4A of the PHA. In doing so, the CPS has ensured that the prosecutors are equipped to charge perpetrators accordingly given that some elements of the newly inserted stalking offences also apply to the activities of cyberstalkers as highlighted in the statutory examples listed under s2A (3) b, c, d, f and g of the PHA. These aspects of the legislation govern the criminal activities of a cyberstalker ranging from the publishing of statements by any means in the name of another person to the monitoring of an individual’s internet usage.

Furthermore, on 20 June 2013 Sir Keir Starmer, the former Director for Public Prosecutions, published guidance on the prosecution of social media cases following a public consultation which commenced in December 2012. The purpose of the guidance was to ensure a consistent approach in the handling of such cases across the CPS. The guidance identified how the threshold will be applied to social media cases.\(^\text{100}\) The CPS guidelines on the prosecution of cases involving social media highlighted the steps that prosecutors are required to take when making decisions that have a social media element. The strengths of the document are that first, it

\(^{100}\) ‘Guidelines on Prosecuting Cases Involving Communication Sent Via Social Media’ (CPS, 2013) <www.cps.gov.uk/legal> accessed 15 June 2017
establishes the grounds for charging defendants and second, it constitutes a point of reference for prosecutors to review and build robust cases against perpetrators.

On 6 October 2014, the CPS updated the legal guidance regarding the prosecution of communication sent via social media. The updated legal guidance explains how current legislation can be used to prosecute offences involving malicious intimate media sometimes referred to revenge pornography.\textsuperscript{101} The guidance was updated further in 2016 to include a section on stalking and was further revised on 21 August 2018.\textsuperscript{102}

In addition to introducing relevant policies to tackle cyber enabled crimes such as cyberstalking, the CPS has taken steps to liaise with other agencies to tackle the issue of stalking and cyberstalking implicitly. Consequently, in September 2016 the former Director for Public Prosecutions confirmed that in July 2015, a stakeholder meeting was held following which, a working group was set up. The working group which consisted of cross government criminal justice specialists and third sector agency representatives explored improvements to the training of prosecutors on stalking.\textsuperscript{103}

In addition to the above, on 23 May 2018 to be precise, the CPS published the updated guidance on stalking and harassment which includes a web-link to the updated protocol on stalking and harassment.\textsuperscript{104} The recent publication demonstrates that the

\begin{flushleft}
\textsuperscript{102} 'Social Media - Guidelines on prosecuting cases involving communications sent via social media' (CPS, 21 August 2018) \textless{}www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media\textgreater{} accessed 11 September 2019
\textsuperscript{104} 'Stalking and Harassment the Crown Prosecution Service' (CPS, 23 May 2018) \textless{}www.cps.gov.uk/legal-guidance/stalking-and-harassment\textgreater{} accessed 13 August 2018
\end{flushleft}
CPS is still taking steps to tackle the criminal behaviour of stalking albeit from a public enlightenment perspective.

1.3.1 Increase in prosecution of stalking cases

On 11 September 2014, the CPS further confirmed that after the first full year of operation, the new legislation resulted in 743 cases being brought to court which would never have been charged under the previous law. Additionally, the CPS confirmed that prosecutions from all stalking and harassment offences using both the new and older legislation, have increased by more than 20 per cent in 2013-14 (from 8,648 in 2012-13 to 10,525 in 2013).105

The data in Table 10 of Appendix 6 indicates that in 2012-2013, the CPS commenced prosecutions in relation to:

- 7,159 offences under S2 PHA 1997 for harassment
- 1,398 offences charged under S4 PHA 1997 for putting people in fear of violence
- 91 prosecutions charged under the new stalking offences:
  - 72 without fear/alarm/distress and 119 involving fear of violence/alarm or distress, since the new offence was introduced in November 2012.

---

Given that the recently created stalking offences include elements of cyberstalking, the data in Table 10 implicitly encompasses cyberstalking.\(^\text{106}\) The data confirms that London prosecutors are utilising the old and new legislation on stalking to prosecute stalkers in absence of a specific legislation on cyberstalking.\(^\text{107}\)

In September 2016, the CPS confirmed that prosecutions were commenced for 12,986 cases involving harassment and stalking offences. The CPS highlighted that this was an increase of 864 offences (7.1\%) from 2014-2015 when 12,122 prosecutions were commenced. The CPS confirmed that this was the highest volume ever recorded.\(^\text{108}\) The CPS additionally confirmed that 1,102 prosecutions were commenced under the new stalking offences (similar to 2014-15 when 1,103 prosecutions commenced).\(^\text{109}\) However in November 2017, the former Director for Public Prosecutions confirmed that in general, there was a decrease in stalking and harassment prosecutions and a rise in prosecution of breaches of restraining orders.\(^\text{110}\)

Despite the above measures which have been implemented by the CPS to promote a consistent approach to the prosecution of stalking and harassment which implicitly includes cyberstalking, on 5 July 2017, Her Majesty’s Inspectorate Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate published critical findings of their joint inspection into how the MET and the CPS tackle the offences of harassment

---

\(^{106}\) On 25 November 2012, the PHA was amended via ss.111 and 112 of the Protection of Freedoms Act 2012. The amendment added two New offences of stalking to the PHA. The first new criminal conduct is the offence of “stalking” as enacted under (s.2A (1). The second New criminal conduct is “stalking involving serious alarm or distress” enacted under (s.4A (b) (ii). Section 2.A (3) gives examples of seven “acts or omissions which in particular circumstances, amount to “stalking”. Although the act gives an exhaustive list of 7 examples of such acts or omission, 5 of the examples relate to the activities carried out by cyberstalkers. These examples are highlighted under (s.2A (3) (b) (c) (d) and (g) respectively

\(^{107}\) The limitation of the data is that it does not indicate how many prosecutions were made in relation to cyberstalking


\(^{109}\) ibid

and stalking offences. The summary of the findings indicate that the CPS and the MET are required to implement additional measures with a view to protecting victims of stalking and harassment and to ensuring that perpetrators are charged with the correct offences.\textsuperscript{111}

The subsequent response of the CPS on 5 July 2017 to Her Majesty’s Joint Inspectorate report is significant. This is due to the fact that the response acknowledged that the CPS needs to implement more measures to improve the services it offers to victims.\textsuperscript{112} Additionally, the response of the CPS identified the measures that the stakeholder will introduce with a view to implementing three of the twelve recommendations which were solely addressed to the CPS and four of the recommendations which were collectively addressed to the CPS and colleagues in the policing sector.\textsuperscript{113} The prompt response of the CPS demonstrates that the stakeholder is keen to act on the recommendations in an attempt to improve the services offered to victims of stalking and harassment which implicitly includes cyberstalking.

From a positive perspective, in September 2018, former Director for Public Prosecutions Alison Saunders revealed that in 2017–18, there was an increase of two thirds in prosecutions commencing under the newer stalking offences.\textsuperscript{114} Additionally, it was confirmed that three quarters of the prosecutions were domestic abuse-related. Also, it was highlighted that more breaches of restraining orders were prosecuted.

\textsuperscript{111} HM Crown Prosecution Service Inspectorate And Her Majesty’s Inspectorate of Constabulary, ‘Living in Fear-The Police and CPS Response to Harassment And Stalking’ (CPS, 2017) <www.living—in fear—the police and cps response to harassment and stalking> accessed 10 July 2017


\textsuperscript{113} ibid

On 12 September 2019, while discussing the latest figures on prosecutions involving Violence against Women and Girls (VAWG), the current Director for Public Prosecutions Max Hill revealed that in 2018-2019, stalking prosecutions increased from 1,616 to 2,209 which was an increase of 36.7% and the highest volume ever recorded.\textsuperscript{115} Additionally, the Director for Public Prosecutions confirmed that the CPS has taken various actions to improve prosecution performance. Notably, it was highlighted that the CPS worked with the National Police Chief Council (NPCC) and College of Policing to provide guidance on harassment and stalking to its police responders.\textsuperscript{116} Additionally, it was also confirmed that a workshop was held by the police and prosecutors to facilitate best practice. Further, it was revealed that the CPS worked with the Home Office and police to develop statutory guidance to support the implementation of the Stalking Protection Act 2019 Act, including a new civil Stalking Protection Order.\textsuperscript{117}

1.4 Response of the Metropolitan Police Service (MPS)

While the CPS introduced relevant policies on stalking and harassment with a view to assisting prosecutors build robust cases against the perpetrators inclusive of cyberstalkers, the MPS took a parallel approach of embarking on an awareness campaign. To this effect, on 18 April 2013 on the National Stalking awareness day, Gary Shewan the UK Lead on stalking and harassment confirmed the following:


\textsuperscript{116} ibid

\textsuperscript{117} ibid
(a) That 20,000 police officers have completed specialist training in stalking developed by the college of policing

(b) That the Metropolitan Police Force had liaised with the Independent Police Complaints Commission and its Continuing Professional Development events to ensure that any lessons on stalking cases are learned

(c) That steps are being made to look at how police forces can be held to account on stalking issues

(d) That the Metropolitan police forces are looking at proposals to develop the national crime recording standards for stalking.

In addition to the above, on 11 September 2014, the CPS and the Association of Chief Police Officers introduced a protocol to ensure a consistent approach to tackling stalking offences. The protocol is an indication that the CPS and the MPS are committed to taking a consistent approach to tackling stalking and cyberstalking implicitly.

Further, to raise public awareness on the issue of stalking and cyberstalking implicitly, on 20 October 2016 the Hampshire Constabulary organised a multi-agency stalking conference. The aim of the one-day conference was to enlighten delegates on the work that is carried out by law enforcement officials at the Hampshire Stalking Clinic who work with offenders with a view to providing rehabilitative treatment. The conference was attended by several representatives of the law enforcement agencies,
academics and victim support groups. The significance of the conference which was attended by the researcher, is that it afforded officials in the psychiatry, police, probation, academic and victim advocacy sectors the opportunity to enlighten delegates on how the clinic works as a multi-agency unit.

The Hampshire Stalking Clinic is a multi-agency forum that meets monthly to review the 4 stalking cases which have generated the highest concern in the county. The three pronged goals of the clinic are to analyse the risks that are created by the stalker, proffer advice to the relevant professionals and offer support to the victims of stalking. The clinic which received government funding has been described as the first of its kind globally given that it has the dual fold goals of enhancing responses to stalking across the criminal justice system in addition to the health sector via the rehabilitative treatment for stalkers. To this effect, on 5 July 2017, it was reported that the Hampshire Stalking Clinic had been recognised as best practice in the national inspection of stalking and harassment. The stalking and harassment service which covers the region of Hampshire was commended by Her Majesty’s Inspectorate of Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate.

In addition to the above on 5 July 2017, David Tucker, the crime and criminal justice lead for the college of policing provided a response to the joint government inspectors on how the organisation tackles the offences of stalking and harassment. In his response, David Tucker acknowledged that stalking and harassment can have a

detrimental impact on an individual’s life and confirmed that training will be introduced for all new police recruits and existing officers. This suggests that as a stakeholder, the MPS like the CPS is willing to implement the recommendations of Her Majesty’s Inspectorate Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate in a bid to tackle the offences of stalking and harassment with a view to improving the services offered to victims of stalking and harassment.

As previously highlighted to improve prosecution performance, the CPS worked with NPCC and College of Policing to provide guidance on harassment and stalking to police officers. Also, a workshop was held by the police to cascade best practice.

In summary, various challenges can hinder police officers and prosecutors from investigating and prosecuting cyberstalkers. The above discussion indicates that the CPS and the MPS are willing to implement recommended measures to enhance the prospects of law enforcement officials successfully bringing offenders to justice.

1.5. Purpose of the current research

The recent cyber-attacks in the UK which affected organisations in at least 100 countries and 48 National Health Service organisations in the UK highlight the Global and instantaneous nature of cybercrime. Since cyberstalking specifically has emerged as an aspect of cybercrime, certain areas of research have been undertaken.

---

126 ibid
The research areas covered include the effects of cyberstalking on victims, the regulation of cyberstalkers, the typology of cyberstalkers and cyberstalking victimisation amongst others. However, limited research investigations have been carried out into the perceptions of police officers and prosecutors in London on cyberstalking victimisation and the threshold of acceptable behaviour on the internet. Further, it has been highlighted that in comparison to offline stalking, cyberstalking has received a lesser attention from the research world.\textsuperscript{128}

Against the above background, there is a research requirement in this area given the recent public concern in the UK over the regulation of cyberstalking. This concern led to a campaign involving the charities Protection against Stalking (PAS) and the National Probation Officers Organisation (NAPO) which resulted in a subsequent consultation with the Home Office. The officials in these organisations, questioned the effectiveness of the PHA legislation as a tool for regulating stalking and implicitly cyberstalking. The public concern reached a climax in February 2012 when the Hon Elfyn Llywd published his findings after being commissioned by the coalition government to chair an independent parliamentary enquiry into stalking law reform.

The primary finding of Elfyn Llywd’s inquiry reiterated the public concern that a specific offence of stalking should be introduced into the legislation of England and Wales.\textsuperscript{129} The question as to whether the public outcry was justified is evident in the subsequent reaction of the coalition government which amended the PHA on 25 November 2012.

The amendment resulted in the addition of two new specific statutory criminal offences under the PHA. The offences are:

(1) “stalking” under s.2A (1) PHA 1997 which is harassment and a conduct that amounts to stalking

(2) “stalking” under s.4a (1) PHA 1997 which can be committed in two ways.

   The first way is “stalking involving fear of violence s.4A (1) (b) (i)

   The second way is “stalking involving serious alarm or distress”, s.4A (1) (b) (ii).

The two new offences were added via s111 and s112 of the Protection from Freedoms Act 2012. Although the amendment did not create a specific statutory offence of cyberstalking, the newly created offences encompass behaviours which may be construed as cyberstalking. The CPS has since confirmed that the new legislation has resulted in more prosecutions in comparison to the old legislation. To this effect, it has launched a new protocol with the Association of Chief Police Officers (ACPO) with a view to ensuring a consistent approach when tackling stalking.

Following the amendment of the PHA, some academics questioned whether it provides an effective protection from cyberstalking. MacEwan contends that the

---

132 ibid
amended PHA legislation in this era of the internet may not be suitable to regulate cyberstalking. MacEwan suggests that there are five primary means of cyberstalking which could indicate that cyberstalking is different from offline stalking even though cyberstalking is sometimes accompanied by offline stalking or results in offline stalking. MacEwan concludes by asserting that although the new offences can regulate certain aspects of cyberstalking, they will not be effective for all aspects of cyberstalking especially if the offences relate to covert activities.

In response to MacEwan’s assertion, Gillespie has counter argued that the amended PHA legislation is effective in protecting victims of cyberstalking.\textsuperscript{134} Gillespie argues that although there are uncertainties to be addressed regarding the creation of two new offences which are solely based on the initial offence of harassment, the PHA has nevertheless, demonstrated that it is flexible especially after the various statutory amendments which have been made to it.

From a different perspective, it has been argued that the new offence of stalking involving alarm or distress created under s.4A (1) b (ii) which has been added to the PHA, is an extra protection for victims given that it looks at the cumulative effects of stalking on a victim as opposed to the effect and characteristics of each individual offence. Addison and Perry contend that the new offence could be a crucial change given that it carries a maximum sentence of five years imprisonment.\textsuperscript{135}

In consideration of the above and given that the debate on cyberstalking seems to focus on the regulation of cyberstalking, the impact of cyberstalking on victims and the

\textsuperscript{135} Neil Addison and Jennifer Perry, ‘Will the New Stalking Legislation Deliver For Victims? (2013) Criminal Law and Justice Weekly 53
public perception of cyberstalking, there is an additional research requirement into the perceptions of police officers and prosecutors on cyberstalking. The research requirement is justified because the findings will enlighten the stakeholders of the policy changes that are required to enable police officers and prosecutors to bring cyberstalkers specifically and cyber criminals in general to justice.

Furthermore, a major interest of the current research was to analyse the responses of the research participants with a view to identifying their perceptions on cyberstalking. Accordingly, the researcher identified the opinions of the participants on the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking.

Against the above background, this thesis highlights six difficulties which the participants perceive that they will likely encounter in the investigation and the prosecution of cyberstalkers and identifies solutions to the highlighted problems. The research will conclude with recommendations addressing the perceived difficulties highlighted.

1.5.1. Structure of the Thesis:

This thesis consists of five chapters.

Chapter One Introduces the research and its current context. To this end it presents and discusses the data from both national and international academic literature on the challenges faced by law enforcement officials in the prosecution of cyberstalkers. Additionally, the jurisdictional, legislative, evidential and financial investigative
impediments to the prosecution of cyberstalkers are examined. Further, the structure and the purpose of the research are identified.

Chapter Two offers a *Review of the literature*, wherein the academic literature is discussed. Specifically, this chapter provides a review of the existing literature in relation to certain key areas, the distinction between cyber-dependent and cyber-enabled crimes, the distinction between cyberstalking and cyberbullying and the regulation of cyberstalking. Additionally, this chapter examines risk assessment of stalking victims, cyberstalking victimisation and police perceptions and the theoretical framework of cyberstalking.

Chapter Three presents the methodology.

Chapter Four presents the results of the analysis of the interview data.

Chapter Five presents the discussion of the findings in relation to both the academic literature and legal theory. Furthermore, it makes recommendations for policy and practice based upon the findings of the thesis.

The next chapter will provide a review of the literature in relation to cyberstalking.
Chapter Two Review of the literature

This chapter offers a review of the existing literature in relation to cyberstalking, the legislation that exists to regulate and counteract it and the mechanisms in place in the UK to prosecute such crimes. The primary purpose of the literature review was to acquire knowledge on the topic with a view to identifying the materials that are relevant to the research questions. The secondary purpose of the literature review was to identify gaps in previous research and to open questions left from other research to ensure the thesis further develops knowledge in the field.

2.1 Literature Review Strategy

The researcher adopted a comprehensive search strategy to carry out the literature review which informs this chapter of the dissertation. The researcher first reviewed and analysed relevant academic literature which were available within the University of West London library. The researcher additionally analysed academic materials then supplemented the research by accessing the SCONUL facility which entitles university members students to access or borrow books from other UK university libraries. The researcher specifically analysed academic materials in the British library and the Institute of Advanced Legal Studies.

In addition, the researcher accessed online search engines such as Google and Yahoo and electronic databases (Lexis Web, All England Law Reports, Justia, Lexis-Nexis, Westlaw and Crime library) with a view to obtaining further relevant literature. The search terms used on the electronic databases comprised a wide variety ranging from independent to combined terms. Some of the terms included ‘cyberstalking and prosecution’, ‘cyberstalking and risk assessment’, ‘cyberstalking and investigation’,
In addition to the above, the relevant policies of the Crown Prosecution Service (CPS) were reviewed. A general search of all relevant websites in the UK was carried out along with English language searches for information about cyberstalking in the UK. Some of the websites include but are not limited to the National Stalking Helpline, Paladin National Stalking Helpline, Paladin National Stalking Advocacy, Protection against Stalking, and Network for Surviving Stalking. The literature review was also compiled by searching relevant textbooks, online newspapers and online journals.

2.2 Definition of cyberstalking

From an academic perspective given that there is no universal definition of cyberstalking, this thesis suggests that an acceptable definition of cyberstalking should contain five elements which would:

1. Identify the deviant behaviours that constitute cyberstalking
2. Identify the means by which cyberstalkers target victims
3. Highlight the effects of cyberstalking on victims
4. Establish a standard test for gauging whether the conduct of a cyberstalker
is as an acceptable behaviour

5 Identify the potential culprits

For the purposes of this study, the researcher has therefore chosen to apply the definition postulated by Bocji and McFarlane. Bocji and McFarlane defined cyberstalking as a collection of behaviours based on which an individual, group of individuals or organisation harass one or more individuals via the use of information and communication technology.

Harassment is defined with a view to establishing whether a reasonable person in possession of the same information about a course of conduct would believe that such conduct would lead another person to experience emotional distress. The distinguishing features of Bocji and McFarlane’s definition are:

(1) The definition highlights that cyberstalking is characterised by a group of behaviours as opposed to just one or two behaviours. This is an important observation which arguably recognizes that the activities engaged in by cyberstalkers comprise of a non-exhaustive list of behaviours.

(2) The definition acknowledges that the cyberstalker could be an individual, a group of individuals or an organisation. This aspect of the definition gives a three-pronged perspective of a possible cyberstalker and is very persuasive given that there is usually an assumption in some available literature that the

---

cyberstalker is an individual as opposed to a group of individuals or an organisation.

(3) The definition distinguishes between information and electronic communication as a means for a perpetrator or perpetrators to harass victims and in doing so, differentiates between the computer-based technologies that may be utilised by a cyberstalker and the communication techniques that may be utilised by a cyberstalker i.e. telephones, computers, fax machines and so on.

(4) The definition identifies the effects of cyberstalking on a victim and in doing so, establishes that there is a causal link between the conduct of a stalker and the resultant effect on a victim.

The above line of reasoning is evident in the recent UK case of Justine Reece who committed suicide on 22 February 2017 after being physically stalked and cyberstalked by her former partner Nicholas Allen for approximately six months. Prior to committing suicide, Ms Reece left a suicide note blaming the actions of her cyberstalker for her decision to take her life. On 28 July 2017, it was reported that Nicholas Allen was sentenced to 10 years imprisonment after pleading guilty to the manslaughter charge and accepting that his campaign of threats and harassment led to the victim’s death.137

(5) The definition, applies the Subjective Test to define harassment as the

---

specific conduct engaged in by a cyberstalker. The test is similar to the test which is applied under s7 (2) of the recently amended PHA.

2.2.1 Definition of cyberstalking as an aspect of cybercrime

Focusing on victimisation, Pittaro asserts that the internet has resulted in the emergence of cyberstalkers. This assertion raises the question of how cyberstalking can be understood within the generic conceptual framework of cybercrime.

Chawki, Darwish, Khan and others suggest that the motives for computer related crimes are revenge, greed, lust, power, adventure and the desire for a thrill. From a victimisation perspective, it could therefore be argued that cyberstalking is a computer enabled crime which enable perpetrators with various motives to utilise various tools such as desktop computers, laptops and mobile phone Wi-Fi devices to victimise others. Consequently, from a psychological perspective, Ahlgrimm and Terrance indicate that cyberstalkers repeatedly pursue victims in a bid to control, intimidate or monitor them utilising electronic or internet technology.

In the absence of a universal definition for cyberstalking, cyberstalking has been defined based on a twofold distinction by the UK government. Notably, in July 2016, the National Cyber Security Strategy defined cybercrime as an offence encompassing the closing linked aspects of cyber-dependent and cyber-enabled crimes.

---

139 Mohamed Chawki, Ashraf Darwish, Mohamed Khan and Sapna Tyagi ‘Cybercrime: Digital Forensics and Jurisdiction’ (2nd ed, OUP) 1
140 ibid
Cyber-dependent crimes are crimes that are mainly aimed at computers or network resources where the devices are both the tool for committing the crime, and the target of the crime. Cyber-dependent crimes are significant because they are symbolically novel crimes - virtual crimes, wherein a digital system is the target as well as the means of attack.\textsuperscript{143} McGuire and Dowling acknowledge that there are various forms of cyber-dependent crimes.\textsuperscript{144} Cyber-dependent crimes encompass a variety of offences ranging from the theft of data to the destruction of computer systems and networks.\textsuperscript{145} Furnell therefore emphasises that the threats posed by hacking and malware specifically which are aspects of cyber-dependent crime have evolved with the passage of time and suggests that updated defences should be developed to reflect the change.\textsuperscript{146}

In comparison to cyber-dependent crimes, cyber-enabled crimes are crimes which can be increased in scale or reach via computers, computer networks or other forms of Information and Communication Technology.\textsuperscript{147} Cyber-enabled crimes encompass several traditional activities. The activities include economic crimes, malicious communications, child sexual offences and extreme pornography among others.

\begin{itemize}
\item \textsuperscript{143} ‘House of Commons Home Affairs Committee E-Crime Fifth Report of Session 2013–14’ (Parliament, 17 July 2013) <www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf> accessed 5 December 2018
\item \textsuperscript{145} Cyber-dependent crimes include hacking, denial of service and botnet attacks. They also include malware attacks such as viruses, trojan horses and spyware
\item \textsuperscript{146} Steven Furnell in ‘Hackers, Viruses and Malicious Software’, Yvonne Jewkes and Majid Yar (eds) \textit{Handbook of internet crime} (Wilan,2010) 173
\end{itemize}
which are committed via the use of Information and Communication Technology.
Applying the above criteria to cyberstalking, cyberstalking can thus be defined as a

cyber-enabled crime. This is due to the fact, that cyberstalking may be viewed as an
aspect of the traditional crime of stalking which can be increased in scale or reach via
the use of computers, computer networks or other forms of Information and
Communication Technology.

The above definition of cybercrime has been applied in its' entirety by the CPS as
highlighted in its published guidance on the prosecution of cybercrime. From a legal
perspective, the implication of this is that the CPS has validated the governments'
definition of cybercrime.

2.2.2. The distinction between offline stalking and cyberstalking

There is currently no consensus on whether cyberstalking should be viewed as an
entirely new form of criminal behaviour, albeit related to offline stalking. The
difference between offline stalking, otherwise referred to as stalking, and cyberstalking
is that offline stalking occurs in the physical realm as opposed to cyberstalking which
occurs in the cyber realm. Stalking has been defined as the intentional, malicious and
repeated pursuit and harassing of another that makes the person fear for his or her
safety. Melroy and Felthouse argue that stalking is generally characterised by the
following three features: acts of unwanted pursuit that occur on more than one

---

149 Suzanne Van der Aa, ’International (Cyber) Stalking, Impediments to Investigation and Prosecution’ (Pure, 1 January 2011) <www.pure.uvt.nl/ws/files/1310512/Aa_International_cyberstalking_110216_posprint_embargo_1_y.pdf > accessed 9 August 2018
150 Reid Melroy and Alan Felthouse ‘Introduction to this Issue: International Perspectives of Stalking’ (Wiley, 2011) <www.pdfs.semanticscholar.org/5a2a/589bc5d273c7462ad6b684bcc73ce820de46.pdf> accessed 6 December 2018
occasion, a credible threat, and the induction of fear in the victim.\textsuperscript{151} To this effect, Worsley, Wheatcroft, Short and Corcoran highlight that the traditional form of stalking is a public health issue and acknowledge that the evolution of the internet has led to the phenomenon of cyberstalking which is a new way of offending.\textsuperscript{152} Consequently, from a law enforcement perspective, Reynolds argues that the crime of stalking in the physical realm has been given another dimension on the internet.\textsuperscript{153} Similarly, Piotrowski and Lathrop highlight that there is a school of thought which argues that cyberstalking is a new form of stalking.\textsuperscript{154}

From a right to free speech perspective, Baer argues that cyberstalking is different from physical stalking because it gives rise to issues which relate to the right to freedom of speech\textsuperscript{155} Baer therefore suggests that law makers and enforcers should apply divergent considerations for identifying and prosecuting cyberstalking. Goodno in comparison, highlights two similarities between stalking and cyberstalking.\textsuperscript{156} The first similarity is that stalkers and cyberstalkers have the common wish to exert control over the victim. The second highlighted similarity is that stalking, and cyberstalking require repeated harassing or threatening behaviour, which is often a start to more serious behaviours. Fundamentally, Goodno goes a step further by identifying 5 differences between stalking and cyberstalking.\textsuperscript{157} Goodno acknowledges that although the offline stalker and the cyberstalker both share a common goal of

\textsuperscript{151} ibid
\textsuperscript{152} Joanne Worsley, Jacqueline Wheatcroft, Emma Short and Rhiannon Corcoran ‘Victims’ Voices: Understanding the Emotional Impact of Cyberstalking and Individual Coping Responses’ (Sage, April 2017) <www.journals.sagepub.com/doi/abs/10.1177/2158244017710292> accessed 7 December 2018
\textsuperscript{154} Peter Piotrowski and Peter Lathrop ‘Cyberstalking and College Students: A Biometric Analysis Across Scholarly Databases’ (2012) 46 College Student Journal 3
\textsuperscript{155} Merritt Baer ‘Cyberstalking and the Internet Landscape We Have Created’ (2010) 15 Virginia Journal of Law and Technology 2
\textsuperscript{156} Naomi Goodno, ‘Cyberstalking a new crime: evaluating the effectiveness of the current federal and state laws’ (2007) 72 MLR 128
\textsuperscript{157} The differences range from the fact that cyberstalkers can instantly harass victims via the internet to the fact that cyberstalkers can offend anonymously
controlling the victim, there are various differences between the two criminal
behaviours which makes stalking a distinct offence from cyberstalking.\textsuperscript{158} Goodno’s
perspective is in contrast to Vasiu and Vasiu’s stance that cyberstalking is construed
by most people as a variant of stalking.\textsuperscript{159}

From an analytical perspective, Chawki like Goodno acknowledges that there are
similarities and differences between stalking and cyberstalking.\textsuperscript{160} Specifically, Chawki
argues that there are 3 specific similarities between cyberstalking and offline stalking
based on the types of victims, the typology of offenders and the motives of the
offenders.\textsuperscript{161}

Sheridan and Grant conducted a research study involving 1,051 self-defined stalking
victims to investigate whether the experience of traditional stalking is distinct from
cyberstalking. They found that there was no fundamental difference based on victim
experience between cyberstalking and the traditional form of stalking in the physical
realm.\textsuperscript{162} Furthermore, Drebing and his colleagues, conducted a research study
based on 6,379 participants and found that victims can experience transitions from
online stalking to offline stalking.\textsuperscript{163} Drebing and his colleagues therefore argued that
cyberstalking is perceived to be a supplementary or similar behaviour to stalking.\textsuperscript{164}

\begin{footnotesize}
\begin{enumerate}
\item Chawki additionally suggests that there are 3 differences between offline stalking and cyber stalking. The differences are that offline stalking requires the victim and the stalker to be in the same geographical area, technologies enable cyberstalkers to target a victim via a third party and a cyberstalker does not need to physically confront the victim
\item Harald DreBing, Josef Bailer, Anne Anders, Henriette Wagner and Christine Gallas, Cyberstalking in A Large Sample of Social Network Users: Prevalence, Characteristics and Impact Upon Victims’ (2014) 17 CBSN 61
\item The aim of the study was to investigate the prevalence of cyberstalking victimization, characteristics of victims and offenders and the impact of cyberstalking on the victim’s well-being and mental health. The research was based on an online survey of 6,379 participants
\end{enumerate}
\end{footnotesize}
Conversely from a victimisation perspective, Alexy, Burgess, Baker and Smoyak conducted a research study involving 756 American university students and concluded that there were differences between stalking and cyberstalking. Specifically, they found that there was a higher occurrence of male cyberstalking victims in comparison to offline stalking victims.

Similarly, Berry and Bainbridge argue that cyberstalking is distinct from offline stalking given that there are different motivations and behaviour patterns. Additionally, Reyns, Henson and Fisher when comparing cyberstalking victimisation to stalking victimisation, investigated the lifetime prevalence of cyberstalking victimisation and cyberstalking offending among a large sample of 974 college students. Significantly, Reyns, Henson and Fisher found that strangers are more prone to offend in cyberstalking cases in comparison to stalking cases. From a clinical, and demographic perspective, Cavezza and McEwan compared 36 cyberstalking offenders with an age and gender matched sample of 36 online offenders. Their research found that there were few differences between cyberstalkers and offline cyberstalkers.

---

166 There were three purposes of this descriptive study. The first purpose was to identify the labels, feelings, and behavioural reactions of college students about cyberstalking. The second purpose was to establish the prevalence and coping mechanisms of cyberstalking victims. The third purpose was to compare the labels, feelings, and behavioural reactions of cyberstalked to stalked victims.
167 Mike Berry and Sonya Bainbridge Manchester’s Cyberstalked 18-30s. Factors Affecting Cyberstalking. 4 Advances in Social Sciences Research Journal 18
168 Bradford Reyns, Billy Henson and Bonnie Fisher ‘Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending among college students’ (2010) 33 DB 1
169 Cristina Cavezza and Troy McEwan ‘Cyberstalking Versus Offline Stalking in a Forensic Sample’ (Researchgate, 2014) <www.researchgate.net/publication/264901467_Cyberstalking_versus_off-line_stalking_in_a_forensic_sample> accessed 9 December 2018
170 Despite the findings, a significant aspect of offline stalking which distinguishes it from cyberstalking is that offline stalking occurs in the physical realm as opposed to cyberstalking which occurs in the virtual or digital realm.
Moreover, from a geographical perspective, Shimzu argues that the borderless and instantaneous access features of cyberstalking are aspects of the conduct which make it distinct from physical stalking.\textsuperscript{171} Shimzu further highlights that another distinguishing feature of cyberstalking is that perpetrators can utilise the internet to urge other people to harass or make threats to the victim.\textsuperscript{172}

The divergent academic evidence outlined above demonstrate that there are two schools of thought on the issue. The first school of thought is that cyberstalking is a distinct behaviour from offline stalking. The second, is that cyberstalking is a supplementary aspect of stalking in the physical realm.

Despite these differing perspectives, a crucial difference between stalking in the physical realm and cyberstalking is that cyberstalkers can use the internet and ICT to victimise instantaneously, speedily, cheaply, anonymously and globally.\textsuperscript{173}

\subsection*{2.2.3 Cyberbullying: A divergent cyber enabled crime analogous to Cyberstalking}

From a general perspective, Caven-Clarke defines cyberbullying as utilisation of the internet, emails, text messages or digital technology to intentionally embarrass or
upset individuals. However, with specific reference to young people, Topaloglu and Topaloglu define cyberbullying as offences such as harassment, humiliation and intimidation of a child or adolescent by other individuals utilising the internet and mobile technologies. Similarly, O’Moore stress that cyberbullying is a common part of bullying amongst children and young people which is committed via technology devices predominantly smart phones and the internet.

From a victimisation perspective, Schwartz notes that cyber bullies create fake websites about their victims asking others to post comments about them. With specific reference to youths, Al-Rahmi and others highlight that new methods of communication have become prevalent among youths Al-Rahmi and others emphasise that smart phones and digital tools can lead to cyberbullying which is dangerous for students. Against this backdrop, Nixon argues that there is a correlation between cyberbullying victimisation and internalising issues and cyberbullying victimisation and externalising issues. Nixon therefore asserts that cyber bulling is a relatively new construct which has become an international public health concern amongst adolescents.

174 Steffi Caven-Clarke ‘Cyber bullying A Focus On’ (1st edn, Book life Publishing 2018) 8
175 Murat Topaloglu and Aysegul Topaloglu ‘Cyber bullying Tendencies of High School Students’ (2016) 15 Int J Edu Sci (1)
176 Mona O’Moore ‘Understanding Cyberbullying’ (1st edn, Veritas 2014) 1
177 Heather Schwartz, Cyberbullying (2nd edn, Raintree 2016) 1
179 The methods of communication are SMS communication, social media platforms, chat forums, emailing, webcams, instant messaging apps and websites.
181 Nixon highlights internalizing issues as the development of negative affective disorders, loneliness, anxiety, depression, suicidal ideation, and somatic symptoms. Nixon further highlights the externalizing issues as the use of drugs, alcohol, carrying of weapons and the display of aggression
From a contrasting perspective, Rogers points out that cyberbullying is different from face to face bullying because cyber bullies can keep a distance between themselves and the victims thereby enabling them to remain anonymous online and having a perceived sense of security that they will not get caught.\textsuperscript{182} Rogers writes from a perspective which suggests that it is difficult to control electronically forwarded documents given that the cyber world enables people globally, to instantly view a single online communication numerous times. Similarly, Hogan argues that cyberbullying is different from traditional bullying because the internet enables cyber bullies to be crueler than they would be in real life.\textsuperscript{183} Additionally, Hayes states that the debate on the difference between cyberbullying and face to face bullying is two-pronged\textsuperscript{184} and that the two-pronged aspects of the debate are significant.\textsuperscript{185}

Notably, Katz emphasises that cyber bulling is characterised by three features.\textsuperscript{186} The features are an imbalance of power which makes it impossible for the victim to defend him/herself, an intention to hurt, humiliate or intimidate the victim and a repletion in a campaign to hurt.\textsuperscript{187} From a comparative perspective, the researcher argues that these three elements of cyberbullying identified by Katz are also features of cyberstalking.

\textsuperscript{182} Vanessa Rogers ‘Cyber bullying’ (1\textsuperscript{st} edn, Jessica Kingsley 2010) 1
\textsuperscript{183} Shanna Hogan ‘Cyber bullying is worse than Traditional Bullying’ in Lauri Friedman (ed) Cyber bullying (Greenhaven Press 2011) 11
\textsuperscript{184} Susan Hayes ‘Cyber bullying is a Serious Problem’ in Lauri Friedman (ed) Cyber bullying (Greenhaven Press 2011) 11
\textsuperscript{185} The first prong is based on the argument that cyber bullying is not as devastating as bullying because victims do not physically interact with the cyber bullies and can be separated from the cyber bullies by turning off their computers. The second prong of the debate is that cyber bullying is worse than traditional bullying because cyber bullies utilize the internet anonymously to intimidate, mock, threaten, embarrass and harass individuals. Additionally, the internet enables people to be more horrid than they would have be in real life.
\textsuperscript{186} Adrienne Katz, ‘Cyber bullying and E-Safety What Educators and Other Professionals Need to Know’ (1\textsuperscript{st} edn, Jessica Kingsley Publishers 2012) 1
\textsuperscript{187} Ibid
2.2.4 Comparisons of Cyberstalking and Cyberbullying

McQuade, Rogers, Genty, and others argue that the internet and the world-wide-web have changed bullying and stalking.\(^{188}\) They highlight that bullies and stalkers are now able to escalate victimisation and to encourage others to join in via the usage of several technological tools.\(^{189}\)

The criminal behaviours of cyberbullying and cyberstalking share five common characteristics. The first shared characteristic is that cyberbullying and cyberstalking are both cyber enabled crimes. The second shared characteristic is that both behaviours can escalate from harassment in the physical realm to harassment in the cyber realm and vice versa. The third shared characteristic is that cyber bullies and cyberstalkers use information and communication technology to target and victimise individuals instantly, cheaply, speedily, anonymously and globally at the click of a button. The fourth shared characteristic of cyberbullying and cyberstalking is that cyberbullying and cyberstalking can affect the health of victims mentally, emotionally, psychologically, physically and sometimes lead to the death of victims either by the victims committing suicide or being murdered by the cyber bullies or cyberstalkers. To this effect, Fahy, Standsfield, Smuk and others examined the longitudinal associations between cyberbullying involvement and adolescent mental health based on a sample of 2,480 teenagers\(^ {190}\) Fahy and others found that there is a high prevalence of cyberbullying and the potential of cyberbullying victimisation as a risk factor for future depressive symptoms, social anxiety and below average well-being among

\(^{188}\) Samuel McQuade, Marcus Rogers, Sarah Genty and Nathan Fisk Cyberstalking and Cyber bullying (1st edn, Chelsea House, 2012) 14

\(^{189}\) The tools include desktops, laptops, computers, cell phones, electronic gambling devices and other mobile computing devices. McQuade, Rogers, Genty and Fisk argue that the tools enable bullies and stalkers victimise and spy on people in person and online using the internet from private or public places thereby breaking down communication barriers.

\(^{190}\) Amanda Fahy, Stephen Stansfield, Melanie Smuk, Neil Smith, Steven Cummins and Charlotte Clarke ‘Longitudinal Associations between Cyber bullying Interactions and Adolescents Mental Health’ (2016) 59 The Journal of Adolescent Health 5
adolescents. Additionally, Betts highlights a case involving a young person whose death was attributed to cyberbullying and negative experiences in the digital world.

Further, Al-Rahmi and his colleagues suggest that cyberbullying is prominent in internet-based harassment and in some cases student suicides.

The fifth shared characteristics of cyberbullying and cyberstalking is that both perpetrators target victims by disseminating harassing messages via electronic communication, posting obscene and disparaging comments on social networking sites and posting humiliating pictures.

Despite the similarities between cyberbullying and cyberstalking a significant difference is that there is a presumption that cyber bulling involves the victimisation of young children as opposed to adults. Consequently, Al-Rahmi and others argue that cyberbullying is different from cyberstalking on two grounds. The first being that cyberbullying usually occurs between minors. The second that cyberbullying is subtler in nature. Similarly, McQuade, Rogers, Genty and Fisk argue that the primary difference between cyberstalking and cyberbullying is that in cyberbullying cases, the victim is known to the perpetrator and usually involves adolescents, whereas in cyberstalking cases the perpetrator is usually an adult with an unknown intent who usually has more menacing motives often sexual in nature. This thesis argues that

---

191 The teenagers were taking part in the Olympic regeneration in East London. Data was gathered from the participants when they were 12 to 13 years old and additionally 1 year after. The purpose was to investigate the link between cyber bullying and future symptoms of depression, social anxiety and overall well-being.

192 Lucy Betts ‘Cyber bullying. Approaches, Consequences and Interventions’ (Palgrave Macmillan, 2016)


195 Samuel McQuade, Marcus Rogers, Sarah Genty and Nathan Fisk ‘Cyberstalking and Cyber bullying’ (1st edn, Chelsea House, 2012)
in cyberbullying cases, the victims sometimes do not know the perpetrators if they are anonymous. The thesis further argues that in some cyberstalking cases, the intent of the cyberstalker is usually apparent especially in cases involving domestic violence. Hence, Miller lists some of the motivations of stalking as a delusional belief in romantic destiny, a desire to reclaim a prior relationship and a sadistic urge to torment the victim out of revenge.196

Furthermore, Katz argues that the rapid development of technology in the last decade has resulted in significant adult concern over the risks facing children from cyberbullying.197 Likewise, Nixon argues that cyberbullying has become so endemic in adolescent experience that they have come to expect and accept cyberbullying.198 Similarly, Phippen acknowledges that cyberbullying is characterised by peer oriented online abuse.199 Therefore, this academic evidence demonstrates that cyberbullying is perceived as an aspect of cybercrime which relates to the victimisation of children as opposed to adults

Considering the above, Hayes argues that cyberbullying is a serious problem on the grounds that increased reports of suicide and school violence appear to be connected to cyberbullying.200 From a criminalisation perspective, Sanchez therefore suggests that cyberbullying should be treated as a crime because some victims end up dead.201

---

197 ibid
198 Adrienne Katz, ‘Cyber bullying and E-Safety What Educators and Other Professionals Need to Know’ (1st edn, Jessica Kingsley Publishers 2012) 1
200 Susan Hayes ‘Cyber bullying is a Serious Problem’ in Lauri Friedman (ed) Cyber bullying (Greenhaven Press 2011) 11
201 Linda Sanchez ‘Cyber bullying should be treated as a crime’ in Lauri Friedman (ed) Cyber bullying (Greenhaven Press 2011) 34
Of more concern are statistics revealed by research carried out in the UK in 2013. The study which was based on a sample of 10,008 young people found that 7 in 10 young people experience cyberbullying and approximately 5.43 million young people in the UK have experienced cyberbullying, with 1.26 million subjected to extreme cyberbullying on a daily basis. Additionally, in 2017 a report highlighted that 1 in 8 young people have been bullied on social media. The report further revealed that 3 in 4 parents have looked for or received information or advice about how to help their child manage online risks. A further report found that 1 in 4 young people have come across racist or hate messages online. The reports reveal that cyberbullying is a cyber-enabled crime which blights the lives of young people in the UK. Additionally, the recent Annual Bullying Survey which was conducted in conjunction with secondary schools and colleges in 2019, revealed that 74% of 2,347 young people experienced cyber bullying between November 2018 and February 2019.

Considering the above, the prevalence of cyberbullying in the UK has led to charitable organisations such as Childline, NSPCC and the Cybersmile foundation implementing measures to increase public awareness on the issues while assisting young victims to cope with the aftermath.

204 The report was based on 1,388 in-home interviews with parents and children aged 5-15, conducted from April-June 2017
From the adult perspective, the crime study for England and Wales indicates that in 2015/16, 4.6% of women and 2.7% of men aged 16-59 were victims of stalking. Additionally, it was revealed that 1 in 10 men and 1 in 5 women will be affected by stalking in their lifetime. Further, the National Stalking Helpline revealed in the year 2015 to 2016, it received 16,000 calls. Crucially, previous data from the Crime Survey of England and Wales revealed that between 2009 and 2012, up to 700,000 women were stalked specifically. Also, the Office for National Statistics Crime Survey for England and Wales provided data on the prevalence of stalking and cyberstalking implicitly among adults aged 16 to 74 in the year ending March 2019. The survey found that 6,144 male adults and 7,397 female adults respectively, experienced stalking in the year ending March 2019 which is a combined total to 13,541.

Significantly, despite the fact that the British Crime Survey in England and Wales estimated that 5 million people experience stalking each year, it has been highlighted that there are no official statistics on the percentage that have been cyberstalked. Consequently, it has been implicitly acknowledged by the government that response to stalking at present can be improved by various agencies working together with a view to protecting victims. Hence, on 10 May 2018, the Metropolitan Police Service launched a global multi-agency specialist unit dedicated to tackling stalking in

207 Mike Berry and Sonya Bainbridge Manchester’s Cyberstalked 18-30s. Factors Affecting Cyberstalking 4 Advances in Social Sciences Research Journal 18
208 ibid
209 ibid
210 Mike Berry and Sonya Bainbridge Manchester’s Cyberstalked 18-30s. Factors Affecting Cyberstalking 4 Advances in Social Sciences Research Journal 18
212 ‘Key Facts and Figures’ (Paladin Service, 2019) <www.paladinservice.co.uk/key-facts-and-figures> accessed 7 March 2019
partnership with Barnet, Enfield and Haringey Mental Health NHS Trust and the Suzy Lamplugh Trust.\textsuperscript{214} Crucially, the \textit{Stalking Threat Assessment Centre} will provide a variety of services from various agencies in a bid to tackle stalking and protect victims through working together collectively.\textsuperscript{215} The researcher anticipates that this measure will help protect victims from cyberstalkers who have mental health issues and persistently offend by offering them the medical and rehabilitative help they need. Additionally, this thesis envisages that the measure will protect victims from stalkers who continue to victimise when imprisoned or continue to target victims after they have been released from prison who may not be deterred by the sanctions that are meted by the criminal justice system.

\subsection*{2.2.5 Cyberstalking victimisation and police perceptions}

The growth and integration of the internet into every aspect of the lives of individuals has facilitated the commission of crimes inclusive of cyberstalking.\textsuperscript{216} Bocji notes that cyberstalkers can harass individuals through the transmission of offensive e-mail messages, identity theft and damage to data or equipment.\textsuperscript{217} From a culpability point of view, Maran and Begotti argue that a factor which contributes to victimisation is that students specifically are not as careful when communicating online with strangers as they would be when communicating in the physical realm.\textsuperscript{218} Consequently, Wright explains that individuals become vulnerable to cyberstalking which can also place

\begin{flushright}
\textsuperscript{214} ‘Specialist multi-agency unit to help tackle stalking launched in London’ (MET, 10 May 2018)  
\textsuperscript{215} ibid
\textsuperscript{216} Bradford Reyns ‘A Situational Crime Prevention Approach to Cyberstalking Victimization: Tactics for Internet Users and Online Place Managers’ 2010, 12 Crime Prevention and Community Safety 2
\textsuperscript{217} Paul Bocji, Mark Griffiths and Leroy McFarlane ‘Cyberstalking a new challenge for criminal law’ (2002) 122 CL
\textsuperscript{218} Daniela Marn and Tatiana Begotti ‘Prevalence of Cyberstalking and Previous Offline Victimization in a Sample of Italian University Students’ (2019) 8 Soc.Sci 1
\end{flushright}
them at risk in the physical realm if they post personal information without thinking of the consequences.\textsuperscript{219}

Against the above backdrop, there have been research studies on cyberstalking victimisation globally. Specifically, Halder investigated cyberstalking victimisation of women in India and the effectiveness of laws.\textsuperscript{220} Halder concludes that cyberstalking is essentially an emotional crime which ought to be dealt with via a restorative process along with a therapeutic jurisprudential approach.\textsuperscript{221} Pereira and Matos on the other hand, examined cyberstalking victimisation and what predicts fear in Portugal utilising a sample of 627 young people \textsuperscript{222} Pereira and Matos found that 61.9 % of the participants were repeat victims of cyberstalkers. From an international perspective Baum, Catalano and Rand conducted a study on cyberstalking victimisation in the US using a nationally representative sample of residents in the US aged 18 years and older based on the National Crime Survey and the Supplemental Victimisation Survey.\textsuperscript{223} Baum, Catalano and Rand found that 14 in every 1000 US adults aged 18 and above had experienced this type of victimisation.

The issue of cyberstalking victimisation has also been investigated by researchers in the UK. Specifically, in 2011 Maple, Short and Brown conducted an online survey on cyberstalking victimisation based on 353 self-participants.\textsuperscript{224} Their study found that

\textsuperscript{219} Michelle Wright ‘Cyberstalking Victimization depression, and academic performance: The role of perceived social support from parents’ (2018) 21 Cyberpsychology, Behaviour, and Social Networking 2

>

\textsuperscript{221} ibid

\textsuperscript{222} Filipa Pereira and Marlene Martos ‘Cyberstalking Victimization: What predicts fear among Portuguese Adolescents?’ 22 European Journal on Criminal Policy and Research 2

\textsuperscript{223} Katrina Baum, Shannon Catalano and Michael Rand ‘Stalking Victimization in the States’ (Victims of crime, 2009) <www.ctimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?dvs=0> accessed 18 March 2019

cyberstalking can have several health impacts on victims and lead to changes in their working life, relationship and finance.\(^{225}\)

In London, to date, there have been no studies on the joint perceptions of police officers and prosecutors on cyberstalking and the threshold of acceptable behaviour on the internet. Instead, there have been related studies on police perceptions of stalking with regards to harassment and the role of victim-offender relationships. To this effect Sheridan, Scott and Nixon examined police officers’ perceptions of harassment in England and Wales utilising a sample of 135 police officers in England and 127 police officers in Scotland.\(^{226}\) They found that certain prejudices existed within the police officer’s perceptions of stalking. Furthermore, that a particular bias exists in that police officers in their sample considered former partners to be less dangerous than those who target strangers or acquaintances contrary to existing researching findings.\(^{227}\) Additionally, Weller, Hope and Sheridan investigated police and public perceptions of stalking with reference to the role of victim-offender relationship utilising a sample of 132 police officers and 225 lay participants.\(^{228}\) They found that in both samples, the extent to which given scenarios were deemed to constitute stalking behaviours were determined by prior victim-stalker relationships.\(^{229}\)

In 2019 a UK study comprising of 165 participants, rated victims of cyber abuse encompassing cyberstalking on measures of direct victim blame and perceived social,

\(^{225}\) The study revealed that 324 out of the 353 participants, 324 stated that they considered that they had experienced some form of harassment through electronic communication


\(^{227}\) ibid


\(^{229}\) Significantly cases involving victimization by strangers were strongly deemed by most to constitute stalking
physical and task attractiveness. The study found that factors such as the volume and source of cyber abuse influences direct victim blame and perceptions of attractiveness. The study, however, did not investigate the joint perceptions of UK police officers and prosecutors on cyberstalking victimisation.

Currently, there is a gap in both academic and public knowledge of police officers and prosecutors’ perception of cyberstalking victimisation in London in respect of the threshold of acceptable behaviour on the internet. This study therefore aimed to make several contributions to the growing research in this area on cyberstalking. Firstly, this study uses a representative collective sample of police officers and prosecutors in London to examine law enforcement perceptions of cyberstalking. Secondly, this study is among the first to examine the joint perceptions of police officers and prosecutors of cyberstalking victimisation and what they consider to be the threshold of acceptable behaviour on the internet. Furthermore, the study investigates the perceptions of police officers and prosecutors on whether the existing legislation on stalking in the UK are effective.

Given that cyberstalking can sometimes escalate to stalking in the physical realm and result in fatalities, there is an onus on police officers and prosecutors from a law enforcement perspective to investigate and prosecute perpetrators in a bid to bring offenders to justice. However, the prospects of police officers and prosecutors successfully investigating and prosecuting cyberstalkers may be determined to an extent, by how law enforcement professionals perceive cyberstalking.

At present, the existing literature on cyberstalking has not specifically addressed from joint investigative and prosecutorial perspectives, perceptions of police officers and prosecutors of cyberstalking victimisation and the thresholds of acceptable behaviour on the internet. On a global scale, researchers have instead, investigated perceptions of cyberstalking in relation to other aspects. Specifically, Alexy, Burgess, Baker and Smoyak examined the perception of cyberstalking among college students, and found that the perpetrator was most likely to be a former intimate partner for those students who had been cyberstalked. Participants consisted of 756 students from two different universities. From a law enforcement perspective, Holt, Bossler and Fitzgerald investigated state and local enforcement perceptions of computer crimes based on the ground that there exists a significant gap in our knowledge of law enforcement agencies. The study found that in general law enforcement agencies have now focused on investigating economic driven computer offences given that local agencies are still investigating sex offences.

From a victimisation perspective, Cass and Rosay investigated college students’ perceptions of criminal justice response to stalking utilising a survey which was administered to 513 undergraduate students. The study made two important findings. The first finding is that the prior relationship and the gender of the target and the offender would have an impact on the decision of the police to arrest. The second

---

232 100 of the students were from a state university and 656 students were from a private university
234 The study analysed the views of 437 state and local law enforcement agents and officers in the US to understand their investigative abilities and views on computer crimes
235 Amy Cass and Andre Rosay ‘College Students Perceptions of Criminal Justice System Responses to Stalking’ (2012) Sex Roles 66 (5-6) 393 The data was collected from 370 responses of law enforcement officers to an electronic survey solicitation administered by the Federal Law Enforcement Training Centre. Solicitation emails were sent to 10,000 individuals in state and local law enforcement agencies across the US
finding was that the gender of the target or the offender would also have an impact on police investigations and the filing of criminal charges given that offenders are often perceived to be males and victims are perceived to be females.

Ahlgrim investigated cyberstalking perceptions with reference to the impact of perpetrator gender and the cyberstalker/victim relationship.\textsuperscript{236} Ahlgrim found that cyberstalking scenarios with a male perpetrator were viewed as more consistent with cyberstalking. Additionally, in relation to perception of victimisation, Ahlgrim established that female cyberstalking victims were attributed less blame than male victims.\textsuperscript{237} Ahlgrim’s findings demonstrate two fundamental points in relation to cyberstalking perceptions. The first point is that gender is a factor which can determine whether an individual is blamed for being victimised. The second point is that gender is a factor which can influence people in deciding whether a cyberstalking incident has occurred.

With the aim of filling some of these existing gaps in knowledge, the researcher interviewed the police officers and prosecutors to discern their perceptions on cyberstalking and what they consider to be the threshold of acceptable behaviour on the internet. In doing so the researcher, adopted an empathetic approach in a bid to understand the shared experiences of the participants and imagine their reality as the primary law enforcement officials in the UK who are tasked with investigating and prosecuting cyberstalkers.\textsuperscript{238}

\textsuperscript{237} Participants of the study comprised of 245 participants comprising of 136 men and 109 women between the ages of 18 and 75 years. The study investigated whether additional factors influenced their personal judgements of criminal justice response to stalking
\textsuperscript{238} The researcher did so by building a rapport with them, listening attentively to the participants during the interviews, feeling their frustrations about investigating and prosecutorial impediments and understanding the various challenges that they face in tackling cyberstalking as perceived by them. This approach enabled the researcher to identify the various perceptions of the participants on the law enforcement
As a CPS employee and a criminal justice insider, the researcher endeavoured to go on a journey with the participants by imaging herself in the position of the participants as they responded to the interview questions. This approach enabled the researcher to understand the frustrations of the participants more. Hence, Gair highlights that empathy enriches qualitative research by promoting the ability to hear, feel, understand and value the accounts of others and to convey the empathetic feelings back to the participant.\textsuperscript{239}

2.3. Regulation of cyberstalking in England and Wales

The internet has enabled people to communicate faster with one another on a global scale. However, the internet has additionally facilitated the harassment of people and organisations online by cybercriminals.\textsuperscript{240} Hyson therefore identifies cyberstalking as a type of cybercrime which can lead to individuals being victimised in various ways such as leaving messages on social media websites, emailing victims and hacking into the accounts of victims.\textsuperscript{241} Furthermore, McQuade highlights that cyberstalkers are the eighth out of twelve categories of cybercriminals who abuse information.\textsuperscript{242}

Cleland argues that the criminal law is a very poor ally for victims of cybercrime.\textsuperscript{243} Cleland writes from a perspective which suggests that the general characteristics of criminal law coupled with the features of digital communication and technology create difficulties that impede the investigation and prosecution of cyberstalkers, victimization and the significance of a victim’s social standing in the investigation process.

\textsuperscript{239} Susan Gair ‘Feeling Their Stories: Contemplating Empathy. Insider/Outsider Positionings and Enriching Qualitative Research’ (2012) QHR 1
\textsuperscript{240} Jeffrey Ross ‘Criminal Investigations: Cybercrime’ (Infobase Publishing, 2010) 30
\textsuperscript{241} Colin Hyson ‘Cybercrime’ (Franklin Watts, 2010) 1
\textsuperscript{242} Samuel McQuade ‘Encyclopaedia of cybercrime (Greenwood Press, 2009)
\textsuperscript{243} Jamie Cleland in Cybercrime and Its Victims Elena Martellozo and Emma Jane (ed) Online Racial Hate Speech (Taylor & Francis Group, 2017)
impediments to responding to cybercrime. Consequently, McQuade asserts that cybercriminals are ahead of the criminal justice officials who seek to respond to and manage cybercrime. Brenner on the other hand, recognizes that there is a tension between the policing of cybercrime and the requirement to respect the privacy rights of individuals.

In respect of the above critical observations regarding the regulation of cybercrime, the researcher discusses how the UK government has utilised criminal law to an extent to regulate cyberstalking as an aspect of cybercrime.

2.3.1. An overview and critique of the Protection from Harassment Act 1997 (PHA)

Historically, the PHA (1997) was enacted to tackle stalking. The legislation, however, did not categorically refer to stalking but instead, introduced two criminal offences of harassment. The first offence is pursuing a course of conduct amounting to harassment and the second offence is putting a person in fear of violence.

From a law enforcement perspective, the PHA was criticized by campaigners including the Protection against Stalking charity on the grounds that it was not effective in dealing with stalking specifically. Consequently in 2011, the coalition government responded to the criticism by commissioning an Independent Parliamentary Inquiry

---

244 The hurdles that are highlighted are establishing the jurisdiction that an offence occurred in, establishing the identity of an anonymity of cybercriminals and impermanent online evidence.
245 Samuel McQuade ‘Understanding and Managing Cybercrime’ (Greenwood Press, 2006)
246 Susan Brenner ‘Cybercrime: Criminal Threats’ (Praeger, 2010) 118
247 The offences were introduced via sections 2 and 6 of the Protection from Harassment Act 1997
into stalking law reform which was chaired by the Rt Hon Elfyn Llwyd. The findings of the report which was published in 2012, were noteworthy as they revealed that the victims of stalking did not have confidence in the criminal justice system. The report therefore recommended in addition to other reforms, that a specific law for stalking should be enacted in England and Wales.

In response to the findings of the Independent Parliamentary Inquiry into stalking law reforms, on 25 November 2012, the government amended the PHA via s111 and s112 of the Protection of Freedoms Act 2012 respectively by introducing two new offences of stalking.

2.3.2. Significance of the expanded Protection from Harassment Act 1997

The amended Protection from Harassment Act introduced two new offences on stalking. The first offence that was created is the offence of “stalking” as provided under s 2A (1) of the PHA. The second offence that was created is “stalking involving fear of violence or serious alarm or distress” as provided under s4A (1) of the PHA.

From a law enforcement perspective, the significance of the expanded legislation is that although cyberstalking is not specifically defined as an offence, the newly created offences on stalking have been drafted broadly to incorporate elements of cyberstalking. The offences are discussed below.

---

249 The offences are “stalking” and ‘stalking involving the fear of violence or serious alarm and distress
250 ibid
251 Section 2A (3) of the Protection from Harassment Act 1997 gives seven examples of acts or omission which amount to stalking. Five of the examples under ss 2A (3) (b) (c) (d) (f) and (g) highlight activities carried out by cyberstalkers
2.3.3. Stalking offence under section 2A

The offence of stalking as provided under s2A of the PHA is defined as pursuing a course of conduct which amounts to harassment and stalking. A person found guilty of this offence is liable on summary conviction, to imprisonment for a term of up to six months or a fine, or both.

From a prosecutorial perspective, the significance of this offence is that it enables prosecutors to charge cyberstalkers with the offence of stalking if there is sufficient evidence to demonstrate that there is a realistic prospect of conviction. From a penal perspective, the expanded legislation may enable judges to deter stalkers and cyberstalkers implicitly by sentencing convicted perpetrators to a maximum of 6 months imprisonment or a fine or both.

2.3.4. Stalking offence under section 4A

Section 4A of the PHA (1997) creates the offence of stalking involving fear of violence or serious alarm or distress. The maximum prison sentence for the offence was doubled to 10 years from 3 April 2017 by the Policing and Crime Act 2017. The legislative amendment was introduced following a campaign by the National Stalking Advocacy Service, Paladin Stalking Charity, and a Ten-Minute Rule Bill introduced in October 2016 by Alex Chalk.

---

252 A course of conduct is the same as defined under section 7 of the PHA 1997 and referred to elsewhere in this guidance
253 Pat Strickland ‘Stalking Developments in The Law’ (Research Briefings, 21 November 2018) <www.researchbriefings.parliament.uk/ResearchBriefing/Summary/SN06261> accessed 16 December 2018
254 ibid
From a penal perspective, the more serious offence of stalking involving fear of violence or serious alarm or distress offence enables judges to deter stalkers by sentencing them to a maximum of 10 years imprisonment, an unlimited fine or both.

The offence of stalking involving fear of violence is significant because the offence can be perpetrated in two ways as provided under sections 4A (1) (b) (i) and 4A (1) (b) (ii) respectively. The first way of committing the offence is by causing a person to fear on at least two occasions that violence will be used. The second way of committing the offence is by causing serious alarm or distress which has a substantial adverse effect on the day to day activities of an individual. The two ways of committing the offence of stalking involving the fear of violence are discussed below.

2.3.5 Stalking involving a fear of violence under section 4A (1) (b) (i)

The offence of stalking involving a fear of violence under section 4A (1) (b) (i) has four parts. The first and second elements of the offence stipulate that there has had to be a course of conduct which causes another to fear that violence will be used against him/her. The third element of the offence specifies that the defendant either knows or ought to know that the course of conduct will cause another to fear that violence will be used against him/her. The fourth part of the offence stipulates that the defendant ought to know that his course of conduct will cause another to fear that violence will be used against them if a reasonable person in possession of the same information would think that the course of conduct would cause the other so to fear on that occasion.
Based on the above, prosecutors will only be able to charge a cyberstalker under s4A (1) (b) (i) of the PHA with the offence of putting a victim in fear of violence via stalking if the four highlighted elements are satisfied.

2.3.6. Stalking Involving Serious alarm or distress 4A (1) (b) (ii)

The offence of stalking involving serious alarm or distress under section 4A (1) (b) (ii) has three distinct elements. The first and second elements specify that there must be a course of conduct which amounts to stalking. The third element stipulates that the stalking conduct either causes another to fear on at least two occasions, that violence will be used against him or her or causes another person serious alarm or distress which has a substantial adverse effect on his or her usual day-to-day activities.

Based on the above, prosecutors will only be able to charge a cyberstalker under s4A (1) (b) (ii) with the offence of stalking involving serious alarm or distress subject to the three highlighted elements being satisfied.

In summary, a stalker and cyberstalker implicitly may face imprisonment for up to ten years or a fine, or both if convicted under section 4A of the Protection from Harassment Act. Additionally, on summary conviction, a person is liable to imprisonment for a term of up to twelve months or a fine, or both.

2.3.7 Legal Issues: Decision to charge and the Threshold Test

The CPS is the prosecuting body in England and Wales. Prosecutors and police officers are required to work jointly during the process of investigating and prosecuting
In criminal cases a decision to charge will be made by either the police or the CPS depending on the category and seriousness of the crime committed if there is a realistic prospect of conviction against an accused on each charge. To ensure that charging decisions are fair and consistent, the Director for Public Prosecutions has published guidance on the charging of cases. The importance of the guidance on charging decisions is twofold in respect of police officers and prosecutors.

Fundamentally, during the investigation process, the police are required to refer certain cases to the CPS for charging decisions if the cases satisfy the Code Test which is a ‘realistic prospect of conviction’. Therefore, there is an onus on the CPS to consider cases that have been referred to it by the police with a view to establishing if the cases satisfy the Full Code Test.

From a legal perspective, once the police refer cases to the CPS for charging advice on serious, complex or contested cases, this may result in the prosecutors instructing the police to provide further evidence before a charging decision can be made and to ensure a successful prosecution. The significance of the advice is that it will bring to completion, cases that cannot be strengthened by further evidence.

---


256 The guidance specifies the cases that are to be charged by the police and the case that are to be charged by the CPS. Specifically, the guidance defines the responsibilities of police officers ranging from the charging of cases to the decision to take no further action. Additionally, the guidance defines the responsibilities of prosecutors ranging from the making of charging decisions to determining whether it is suitable to apply the Threshold test in cases where prosecutors are responsible for making charging decisions.

257 In relation to police officers, the charging guidance is significant because it highlights the duty of police officers to investigate offences, assess evidence before charging or referring cases to the CPS and defines the requirement on police officers to refer cases to the CPS. In relation to prosecutors, the Charging guidance is significant because it specifies the duty of prosecutors to assess the evidence provided by the police, highlights the duty to provide early investigative advice in certain cases and defines the requirement in all cases to meet the full code test.

2.3.8. Legal Issues: The Full Code Test

The Full Code Test is set out in the Code for Crown Prosecutors. It is a two staged process which must be applied by police officers and prosecutors prior to making charging decisions. The first stage is the evidential stage and the second stage is the public interest stage. Under the Evidential Test, prosecutors must be satisfied that there is sufficient evidence to provide a realistic prospect of conviction against each suspect on each charge.

The evidential stage of the Full Code Test requires prosecutors to ascertain whether the evidence can be used in court, whether the evidence is credible, whether the evidence is reliable and whether there is any other information that might affect the sufficiency of the evidence. Additionally, the Evidential Test requires prosecutors to examine what the defence case may be, and how it is likely to affect the prospects of conviction. A case which does not satisfy the Evidential Test will not proceed to the next stage.

The Public Interest Test requires police officers and prosecutors to carefully weigh up the factors for and against prosecution prior to establishing how fundamental each factor is in the circumstances of a case and then make an overall assessment.

---


260 ibid

261 ibid

262 The evidential test requires police officers and prosecutors to consider two point. The first point is whether a court or jury is more likely to convict a suspect based in the available evidence. The second point is the effect of any likely defence


There are seven public interest factors which can affect the decision to prosecute. The public interest factors are the seriousness of the offence, the suspect’s culpability, the circumstances of and harm caused to the victim, the suspect’s age and maturity at the time of the offence, impact on the community, whether prosecution is a proportionate response and whether sources of information require protecting.

In certain situations where the Full Code Test is not met, the Threshold Test may be applied to charge a suspect. Specifically, the Threshold Test will only be justified if the seriousness or circumstances of the case warrants the making of an immediate charging decision. Additionally, there must be substantial grounds for objecting to bail. Fundamentally, there are five conditions of the Threshold Test that have to be met to guarantee that the Threshold Test is only applied when required and that cases are not charged too soon. The five conditions of the Threshold Test will need to be satisfied for a suspect to be charged. The first condition is that there are reasonable grounds to suspect that the person to be charged has committed the offence. The second test is that further evidence can be obtained to provide a realistic prospect of conviction. The third condition is that the seriousness or circumstances of a case justifies the making of an immediate charging decision. The fourth condition is that there is continuing substantial grounds for objecting to bail. The fifth condition is that it is in the public interest.

---

265 The public interest factors are the seriousness of the offence, the suspect’s culpability. The circumstances of and harm caused to the victim, the suspect’s age and maturity at the time of the offence, impact on the community, whether prosecution is a proportionate response and whether sources of information and national security will be harmed
267 ibid
268 ibid
2.3.9. The implication of legal issues under the Full Code Test and the Threshold Test on the prosecution of cyberstalkers

The CPS is legally required to make decisions about cyberstalking cases in accordance with the code for Crown Prosecutors to determine whether there is a realistic prospect of conviction. Consequently, the legal issues discussed above may have an implication on the pre-charge decisions and the charging decisions that are made by the police officers and prosecutors respectively.

From a pre-charge perspective, the implication of the legal issues identified above is that certain cyberstalking cases which have been referred to the CPS by the police for a pre-charge advice may be concluded if further evidence will either not strengthen such cases or lead to successful outcomes. This is arguably more so in cases involving anonymous cyberstalkers or cyberstalkers via proxy whose veils of anonymity cannot be unmasked either by the police or by the ISPs.

From an evidential perspective, the Evidential Test will require police officers and prosecutors to consider whether a court or jury is more likely to convict a cyberstalker of a charge after hearing the evidence. Additionally, the Evidential Test requires police officers and prosecutors to consider the effect of any likely defence or information from a cyberstalker’s defence team. Given that there are various evidential difficulties which could impede the investigation of cyberstalkers, police officers and prosecutors may be unable to meet the evidential threshold of a realistic prospect of conviction in cases that are evidentially weak which do not connect a cyberstalker to

---

269 If police officers or prosecutors decide that a court or jury is more likely than not to convict a cyberstalker of a charge after hearing the evidence, then the evidential evidence will be met and they can proceed to consider the public interest test.
a charge. Crucially, a cyberstalking case which does not pass the evidential stage will not proceed, no matter how serious or sensitive it may be.

From a public interest perspective, in every cyberstalking case where there is sufficient evidence to justify a prosecution, prosecutors will then proceed to consider whether a prosecution is required in the public interest. In effect, a cyberstalker will be prosecuted unless the prosecutor is satisfied that there are public interest factors tending against prosecution which outweigh those leaning in favour of a prosecution ranging from the seriousness of the offence to the age and maturity of the cyberstalker at the time of the offence.

In addition to the above, police officers and prosecutors will be unable to apply the Threshold Test to a cyberstalking case if the prerequisite 5 conditions are not met.

2.3.10. Legal issue- Meeting the Reasonable Person Test

The legal issue that may be faced by judges is establishing how the Reasonable Person Test can be effectively applied to determine whether a reasonable person in possession of the same information as a stalker, would have known that his or her conduct will firstly cause a victim to fear that violence will be used against them or secondly cause a victim serious alarm or distress.

A further legal issue which may arise is identifying how stalking can have a substantially adverse effect on the day-to-day activities of the victims given that the phrase has not been defined under section 4A of the PHA. Consequently, the Home Office has outlined six examples of lifestyle changes which may constitute evidence
of the substantial adverse effects that stalking has on individuals.\textsuperscript{270} Specifically, this highlights that the evidence ranges from the victim changing their routes to work to the victim stopping or changing the way they socialise. Significantly, the Home Office acknowledges that the adverse effects may relate to cyberstalking too.\textsuperscript{271}

\section*{2.3.11 Legal Issues-Defining cyberstalking implicitly and a course of conduct}

In the current legislative landscape, the PHA does not legally define stalking and cyberstalking implicitly. Instead, section 2A (3) of the act lists seven behaviours that may be construed as stalking and cyberstalking implicitly.\textsuperscript{272} Specifically, the second, third, fourth and sixth listed behaviours implicitly relate to cyberstalking.\textsuperscript{273}

Given that s.2A(3) is not an exhaustive list and that the courts are required to consider other acts by a defendant and determine whether those acts constitute stalking, a legal issue which may arise in the prosecution of stalkers and cyberstalkers implicitly is that some lawyers representing cyberstalkers lawyers may argue that certain behaviours associated with stalking should be classified as harassment and not stalking.\textsuperscript{274} This legal issue could result in the lawyers therefore arguing that the cyberstalkers are guilty of harassment and not stalking.


\textsuperscript{272} ‘Stalking and Harassment’ (CPS, 23 May 2018) <www.cps.gov.uk/legal-guidance/stalking-and-harassment> accessed 1 January 2018

\textsuperscript{273} The behaviours are contacting or attempting to contact a person by any means, publishing a statement or material either relating to a person or purporting to originate from a person, monitoring the use by a person of the internet, email or any other form of electronic communication and interfering with property of an individual.

\textsuperscript{274} Section of the Protection from Harassment Act 1997 specifies the elements of the harassment offence as a course of conduct which amounts to harassment and the defendant knew or ought to have known that the conduct amounts to the harassment of another
In addition to the above, section 7 of the PHA stipulates that a person will be found guilty if omissions have caused a victim to be in fear of violence on two or more occasions.\textsuperscript{275} The Act however, does not define the length of time that should pass between stalking incidents. This legal issue might, therefore, make it difficult for judges to establish what constitutes a course of conduct when determining cases that are characterised by cyberstalking incidents that are distant apart. Against this backdrop, it has been suggested that certain behaviours may be distant apart and still constitute a course of conduct given that every case will be determined on its own facts.\textsuperscript{276}

In September 2018, the Crown Prosecution Service published statistics on prosecutions for stalking offences in its annual \textit{Violence against Women and Girls report}. The eleventh report significantly indicates that in 2017-18, 1,616 prosecutions were started for stalking offences which is a 68.5 per cent increase from 959 in 2016-17. As previously highlighted (Chapter 1, section 1.3) on 12 September 2019, while discussing the latest figures on prosecutions involving Violence against Women and Girls (VAWG), the current Director for Public Prosecutions Max Hill revealed that in 2018-2019, stalking prosecutions increased from 1,616 to 2,209 which was an increase of 36.7% and the highest volume ever recorded.\textsuperscript{277}

The above statistical data is important because it demonstrates that the CPS and the police are working jointly together with a view to investigating and prosecuting stalkers

\textsuperscript{275} Section 7 defines a course of conduct as being on at least two occasions
\textsuperscript{276} Stalking and Harassment’ (CPS, 23 May 2018) <www.cps.gov.uk/legal-guidance/stalking-and-harassment> accessed 1 January 2018
and cyberstalkers implicitly. The data further indicates that the CPS and the police are prosecuting stalkers despite the highlighted legal issues.\(^{278}\)

In summary, the two stalking offences which have been introduced in the PHA can be used by police officers and prosecutors to bring stalkers, and cyberstalkers implicitly, to justice given that some countries are yet to regulate stalking and may not perceive stalking and cyberstalking as serious offences which warrant a specific legislation.

### 2.3.12 Regulation of cyberstalking which involves hate speech crimes

Hate crimes can be defined as offences which are motivated by any form of discrimination against the victim's ethnic or national origin, gender, disability, age, religion or belief, sexual orientation or gender identity.\(^{279}\) Hate crime occurs if victims are subjected to hostile treatments on the above highlighted grounds. The required evidence of hostility can be obtained via face to face communication, written communication and online or social media communication.\(^{280}\)

Applying the above definition of hate crimes to cyberstalking, cyberstalking can be regarded as a hate crime if a cyberstalker’s hate speech was motivated by any form of discrimination against the victim's ethnic origin, national origin, gender, disability, age, religion, belief, sexual orientation or gender identity.

---

\(^{278}\) The researcher anticipates that there will be a consistent rise in the number of prosecutions if to the CPS and the police continue to work together in a bid to prosecute stalkers


Yar highlights that the criminalisation of hate speech is controversial due to the fact that critics may argue that it will lead to an infringement of the freedom of expression on the internet.\textsuperscript{281} Yar makes his argument from a perspective which indicates that the criminalisation of hate speech could lead to political, journalistic academic and artistic censorship.\textsuperscript{282} However, from a punitive perspective, it can be counter argued that if hate speech is not regulated, it could result in criminals like cyberstalkers victimizing individuals and not being held accountable for their actions.

From a judicial perspective, Baer suggests that if cyberstalking involves threats, the result of a claim concerning a criminal threat is dependent on the contents of the speech and the standards applied by the courts to consider the likelihood and depth of the harm threatened.\textsuperscript{283} Baer therefore, makes a distinction between threats that will be deemed a greater danger and threats which are merely generalized and are proposing intangible harm.

The following four aspects of hate crime that have been regulated in England and Wales are:

1. racially and religiously aggravated crimes
2. homophobic crimes
3. biphobic and transphobic crimes
4. disability hate crime crimes\textsuperscript{284}

\textsuperscript{281} Majid Yar, Cybercrime and Society (2\textsuperscript{nd} edn, Sage 2013)
\textsuperscript{282} ibid
\textsuperscript{283} Merritt Baer ‘Cyberstalking and the Internet Landscape we Have Created’ (2010) 15 Virginia Journal of Law and Technology 2
\textsuperscript{284} ‘Hate Crime’ (CPS) <www.cps.gov.uk/hate-crime> accessed 18 January 2019
From a legal perspective, sections 28 to 32 of the Crime and Disorder Act 1998 and sections 145 and 146 of the Criminal Justice Act 2003 respectively, empower prosecutors to apply for an uplift in the sentence of those convicted of hate crimes. This means that because of the serious nature of hate crimes, the CPS can apply to the courts for a sentence uplift which is an increased punishment for a crime. The implied implication of the legislative provisions with reference to cyberstalking via hate speech is that on conviction, a cyberstalker may receive a higher sentence for demonstrating hostility to a victim based on the victim’s race, religion, disability, sexual orientation or transgender identity.

From a prosecutorial perspective, on 18 October 2018, the CPS confirmed that in 2016/17, 83% of hate crimes cases that were prosecuted led to a conviction or guilty plea. The CPS further confirmed that in 2017, more than half of the organisation’s requests for a sentence uplift led to offenders having their sentence increased because it was motivated by hate.

From a historical perspective, in March in 2012, the Law Commission published the Government’s Hate Crime Action Plan which described its three key principles. The principles are preventing hate crimes, increasing reporting and access to support and improving the operational response to hate crimes. In addition to the above, in 2016

---

286 This is due to the fact that given the serious nature of these offences, the CPS can apply to the courts for a ‘sentence uplift’ which is an increased punishment for the crime.
287 ibid
289 The reason for this legislative action was because the government felt that at the time of the publication of the Law Commission’s action plan, existing criminal offences dealing specifically with hate crimes specifically, did not recognize the five protected prejudicial grounds that motivate offenders which are race, religion, sexual orientation, disability or transgender identity.
the government published an action plan to tackle hate crime. The plan focused on five themes. The first theme is preventing hate crime by challenging beliefs and attitudes. The second theme is responding to hate crime within our communities. The third theme is increasing the reporting of hate crime. The fourth theme is improving support for victims of hate crime. The fifth theme is building the understanding of hate crime.

The CPS has since confirmed that it has implemented the Hate Crime Strategy for the specific period of 2017 to 2020. The two-pronged aim of the strategy is to obtain justice for victims of hate crimes and support everyone thus affected. The strategy highlights the aims and the key commitments of the CPS towards the tackling of hate crimes. Additionally, the CPS has revealed that in April 2020, the CPS will publish its new strategy, ‘CPS 2025’. It is anticipated that the strategy will set out the CPS vision and aims over the next five years and that the CPS’ equality and diversity objectives will be integrated into the strategic framework, and through their annual business planning and reporting cycle. Therefore, the CPS has confirmed that it will report on the progress made against each of their strategic aims.

Significantly, in October 2018 Alison Saunders the former Director for Public Prosecutions confirmed that the recorded sentence uplift increased to 67.1% which

---


293 ibid


295 ibid
exceeds the level of ambition which was set in the CPS 2020 business plan.\textsuperscript{296} Notably, in the Hate Crime Report 2018-2019 which was published on 25 October 2019, the Director for Public Prosecutions Max Hill confirmed that the CPS in hate crime cases, ask the court for an increased sentence or sentence uplift to reflect the additional level of seriousness.\textsuperscript{297} Further, the Director for Public Prosecutions confirmed that in 2018-19, the number of convictions where the court announced a sentence uplift reached the highest level yet at 73.6\%.\textsuperscript{298}

From a privacy perspective, a cyberstalker may decide to argue that his right to freedom of expression has been infringed under Article 10 of the European Convention of Human Rights if he has been convicted of a hate speech based on the racial or religious grounds. However, in the case of DPP v Collins, the court held that a person can be prosecuted for using communications system to leave racist messages.\textsuperscript{299} The significance of this case is that it prevents criminals like cyberstalkers who have been convicted of racist or religious hate crime speech offences from arguing that their rights to freedom of expression as guaranteed by Article 10 of the European Convention on human rights have been infringed. Additionally, it may be difficult for a cyberstalker to prove that hate speech is a protected speech. This is due to the fact that Article 10 is a qualified right which provides that an individual's right to freedom of expression can be lawfully restricted in certain circumstances.\textsuperscript{300} The circumstances are if it is in the interests of public safety or if restriction is required for the protection of the rights and freedoms of others.

\textsuperscript{298} ibid
\textsuperscript{299} [2006] 1.WLR 2223 (QBD)
2. 4 Theoretical framework- Application of traditional criminological theories to cybercrime

Historically, traditional criminological theories have been used to explain the reasons behind traditional behaviour. The development of the internet has however, created challenges in applying traditional criminological theories to cyber space because Cyber space is characterised by architectural and societal hallmarks which differ significantly from the environments in the physical realm.

A specific criminological challenge in applying traditional criminological theories to cyber space is establishing where a cybercrime offence occurs given that traditional criminological theories assume that crimes occur in distinct local environments. Consequently, Stalder highlights that there is no distance at all in cyber space. In this context, D’ Ovidio, Mitman, Jamillah and El-Burki emphasise that computer networks including the internet have reduced the impact of time and space on social interactions. D’ Ovidio, Mitman, Jamillah and El-Burki further stress that the disembodiment of humans and the resulting cyber communication via virtual communities has challenged the traditional concept that communities consist of people and entities that are connected by geographical proximity.

Within the above framework, Yar points out that cyber space cannot be divided into geographical locations in comparison to the real world where geographical distinctions, for example, can be made between neighbourhoods and districts. Yar therefore concludes that the issue of establishing where crimes occurs in cyber space

303 ibid
304 Majid Yar, ‘Cybercrime and Society’ (2nd edn, Sage 2013)
demonstrates that applying criminological views found on spatial divergence can be of limited use.

In relation to cyberstalking, the researcher examined four traditional criminological theories and two modern criminological cybercrime theories in a bid to identify a theoretical schema that can explain cyberstalking victimisation. The traditional theories are the social learning theory, self-control theory, lifestyle theory and the routine activity theory. The two modern theories are the space transition theory and cyberlifestyle routine activity theory. A review of these theories follows.

2.4.1 Self-Control Theory: A theoretical application to cyberstalking victimisation

The general theory of crime was postulated in 1990 by Gottfredson and Hirschi and posits that low self-control is the primary factor that causes crime and deviance.\textsuperscript{305} Gottfredson and Hirschi suggest that the theory consists of six personality traits which collectively determine if individuals tend to commit crimes.\textsuperscript{306}

From a victimisation perspective, Baek, Losavio and Higgins applied the general theory of crime to online harassment to ascertain if adolescents with low level of self-control will be more likely to commit online harassment than those with high level of self-control.\textsuperscript{307} Baek, Losavio and Higgins found that adolescents with low levels of self-control were more likely to commit online harassment than those with high levels

\textsuperscript{305} Fawn Ngo and Raymond Paternoster ‘Cybercrime Victimization: An Examination of Individuals and Situational Level Factors’ (2011) 5 International Journal of Cyber Criminology 1

\textsuperscript{306} The six personality traits of the self-control theory are impulsivity, risk seeking, self-centredness, bad humour and a preference for simple, physical activities

of self-control.\textsuperscript{308} Similarly, Donner and others found that there is a connection between self-control and various forms of online behaviours such as threatening or insulting others through email or instant messaging.\textsuperscript{309} Likewise, Reyns, Fisher and Randa investigated cyberstalking victimisation among 1,987 college students by applying three theories which included the self-control theory.\textsuperscript{310} The study revealed that the self-control theory is one of three theories that can be used to explain cyberstalking victimisation.\textsuperscript{311}

Collectively, the above findings suggest that online harassment in general and Cyberstalking victimisation in particular may be explained from the theoretical lens of the self-control theory.

\textbf{2.4.2 Social learning and behavioural theories of crime: Theoretical applications to cyberstalking victimisation}

The Social Learning theory posits that crime and deviance are learned responses. The hypothesis can be traced to the differential association theory which was postulated by Edwin Sutherland in 1947.\textsuperscript{312} The sociological theory postulates that crime is a social product which is learnt from several social interactions in personal groups or social settings.\textsuperscript{313}

\begin{flushright}
\textsuperscript{308} The sample size was 1,0971 and the data was collected by the Korean Institute of Criminology. The data was based on self-reports surveys collected from school children
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\textsuperscript{310} Bradford Reyns, Bonnie Fisher and Ryan Randa ‘Explaining Cyberstalking Victimization Against College Women Using a Multitheoretical Approach: Self-Control, Opportunity and Control balance’ (2018) 64 Crime and Delinquency 13
\end{flushright}

\begin{flushright}
\textsuperscript{311} The additional theories are opportunity and control balance
\end{flushright}

\begin{flushright}
\textsuperscript{312} Chris Hale, Keith Hayward, Azrini Wahidin and Emma Wincup ‘Criminology’ (3rd edn, Oxford University Press 2013) 124
\end{flushright}

\begin{flushright}
\textsuperscript{313} According to the differential association theory, individuals who associate with groups or communities that either have criminal traits or are isolated from more positive law abiding traits and views will result in the individuals being taught the skills, motivations and beliefs that promote crime and deviance
\end{flushright}
From a psychological perspective, Albert Bandura posited the social learning theory which proposes that new patterns of behaviour can be learned through direct experience or by observing the behaviour of others.\textsuperscript{314} The theory suggests that individuals learn from their interactions with others in a social context specifically via observation, imitation and modelling. Bandura’s observations are significant because they demonstrate that the replication of deviant behaviours was more likely to occur when the actor admired the person who had originally demonstrated the behaviour. Applying this line of reasoning to cyberstalking, it can be argued that cyberstalkers may imitate other perpetrators who they have read about in the press or on the internet and whom they admire having observed them. Based on Bandura’s theory, it follows that cyberstalkers are more likely to offend if they observe other actors, retain knowledge on the observed deviant cyberstalking acts and then being motivated reproduce such acts.

Therefore, it may be considered that offenders engage in cyberstalking activities after observing and imitating the behaviours of other cyberstalkers. This argument is however flawed because it cannot be used to explain cases involving cyberstalkers who have not engaged in offending after observing and imitating others but have instead, victimised former partners or complete strangers independently.

From an empirical perspective, there does not appear to be a body of work in relation to cyberstalking.\textsuperscript{315} Consequently, Fox, Nobles and Akers emphasise that their study


\textsuperscript{315} Kathleen Fox, Matt Nobles and Ronald Akers Is stalking a learned phenomenon? An empirical test of social learning theory’ (2011) 39 Journal of Criminal Justice 1 <https://pdfs.semanticscholar.org/816a/a39206a1dd4a28882464a7c83c4f6baac1.pdf> 27 December 2018
of stalking victimisation within the framework of social learning theory is the first study on stalking perpetration.\textsuperscript{316} From an analytical perspective, Munro and Jeffrey acknowledge that the social learning theory has been referred to as a bridge between behaviourist and cognitive learning theories because the theory encompasses attention, memory, and motivation.\textsuperscript{317} However, Munro and Jeffrey argue that the Social Learning theory has conceptual weaknesses due to the fact that it is difficult to measure social learning either as a process or an outcome.

Nabavi on the other hand, acknowledges that the Social Cognitive Learning theory is derived from the Social Learning theory.\textsuperscript{318} The Social Cognitive Learning theory posits that people learn by observing the actions of others and that the human thought process is the key to understanding personality. From a critical perspective too, Nabavi equally emphasises that the Social Cognitive Learning theory has several strengths and weakness.\textsuperscript{319} Some of the strengths of the theory are the collection of a magnificent accumulated research record, the theory is open to change because it is evolving and the theory focuses on fundamental human social behaviours. These strengths of the theory relate to the research because the accumulated research record validates the application of this theory to the study. Additionally, the theory can be used to explain the worrying human social behaviour of cyberstalking. Some of the weaknesses of the Social Cognitive Learning theory are that some academics consider it to be a loosely organised theory, the theory is based on initial findings and

\textsuperscript{316} Fox, Nobles and Akers investigated the extent to which components of social learning theory namely definitions, differential reinforcement, and differential association or modelling predict stalking victimization. The sample comprised of 2,766 college students. In relation to stalking perpetration and victimization, Fox, Nobles and Akers found that via interaction with peers primarily, behaviours are learned, modified, or reinforced.


\textsuperscript{319} ibid
the theory fails to consider two factors. The first factor is maturity and changes over a lifespan. The second factor is that little attention is paid to motivation, conflict and emotions.

2.4.3 Space Transition Theory: A theoretical application to cyberstalking victimisation

The space theory was developed by Jaishankar in 2008 to explain the causation of cybercrime. The theory posits that people behave differently when they move from the physical space to the cyber space. The space transition theory has seven principles based on which it is suggested that people act differently when they move from one space to another. Danquah and Longe conducted research to ascertain if the postulates of the space transition theory constituted a logical and credible basis for predicting and determining the cause of cybercrime. Danquah and Longe found that the space transition theory is not applicable to all categories of cybercrime.

The first and second postulates of the space transition theory specifically may be significant in examining cyberstalking as an aspect of cybercrime. The first postulate of the space transition theory suggests that people with repressed behaviour in the physical realm have tendencies to commit crime in cyber space which they would not otherwise, commit in the physical realm. Based on the first postulate of the space

---

321 ibid
323 ibid

102
transition theory, it can be argued that cyberstalkers are individuals with repressed criminal behaviour in the physical realm who have the propensity to victimising behaviours in cyber space which they would not otherwise commit in physical space. The researcher however suggests that it may be problematic to strictly apply the first postulate of the space transition theory to cyberstalking given that sometimes, cyberstalkers have the propensity to victimise in the physical realm in addition to the cyber realm. Crucially, some cyberstalkers victimise in the physical realm prior to targeting individuals in the cyber realm and vice versa.

The second postulate of the theory highlights that identity flexibility, dissociative anonymity and a lack of deterrence factor in the cyber realm enable perpetrators to commit cybercrimes. The second postulate of the space transition theory may be equally relevant to cyberstalking victimisation given that the three theoretical features of identity flexibility, anonymity and the absence of deterrent factors enable cyberstalkers to offend. From a law enforcement perspective, the three factors can constitute investigative difficulties which may impede the prosecution of cyberstalkers.

2.4.4 Lifestyle Exposure Theory and Routine Activity Theory: Theoretical Frameworks Applied to cyberstalking victimisation

The Lifestyle exposure theory of victimisation was postulated by Handling in 1978. The theory posits that an individual’s daily activities contribute to victimisation. 


\[325\] Handling highlights that vocational activities and leisure activities are the specific elements of a lifestyle that have a direct effect on the degree of exposure to the level of victimization risk

103
Lifestyle Exposure theory further suggests that the decision to engage in risky activities can be arrived at through individual rational choice.\textsuperscript{326} Against this backdrop, Reyns, Henson and Fisher found that individuals who engage in risky online behaviours such as opening numerous social networks accounts and connecting to strangers were more likely to be victimised.\textsuperscript{327} The theory may be used to explain cyberstalking victimisation based on the argument that individuals may expose themselves to victimisation if they engage in risky activities on the internet.

Support for the notion of victimisation by prior romantic partners is proved by Wick, Nagoshi, Basham and colleagues who conducted research which was based on a sample of 298 college students who completed an online survey about their experiences of being victimised. The research found that the Routine Activity theory can be partially used to explain victimisation and perpetration of cyber harassment by romantic partners.\textsuperscript{328} Specifically, the study found that victimisation for women was associated with greater general risk-taking propensity and online exposure.\textsuperscript{329}

The Routine Activity theory was proposed by Cohen and Felson in 1979.\textsuperscript{330} In comparison, to the Lifestyle Exposure theory, the Routine Activity theory suggests that the probability of victimisation occurring is contingent on three factors. If the three factors synchronize in a given space and time.\textsuperscript{331} The factors are the presence of a

\textsuperscript{326} ibid
\textsuperscript{327} Billy Henson, Bradford Reynolds and Bonnie Fisher ‘Security in the 21st Century: Examining the Link Between Online Social Network Activity, Privacy and Interpersonal Victimization’ (2011) 36 Criminal Justice Review 3
\textsuperscript{328} Elizabeth Wick, Craig Nagoshi, Randy Basham, Catheleen Jordan, Youn Kyoun Kim, Anh Phuong Nguyen and Peter Lehmann ‘Patterns of Cyber Harassment and Perpetration among College Students in the United States: A Test of Routine Activities Theory’ (2017) 11 International Journal of Cyber Criminology 1
\textsuperscript{329} ibid
\textsuperscript{330} ibid
\textsuperscript{331} ibid
motivated offender, a requisite victim and the absence of capable guardians.\textsuperscript{332} Within this framework, Choi argues that this theory is an extension of the Lifestyle Exposure theory postulated by Handling and others on the grounds that it adopts the theoretical principle of the Lifestyle Exposure theory.\textsuperscript{333} Choi based his argument on the findings of a study which applied the Routine Activity theory to computer-crime victimisation.\textsuperscript{334} The Routine Activity theory is therefore considered an extension of the Lifestyle exposure theory of victimisation which focuses on the vocational or leisure activities of individuals.\textsuperscript{335}

Considering the above, it is proffered that the Routine Activity theory may be applied to the cyberstalking victimisation model based on a three-fold construct. The first theoretical construct grounded in the Routine Activity theory with reference to cyberstalking victimisation is that the cyberworld constitutes an environment for several cyberstalkers to look for cyberstalking victims who are suitable targets. To this effect, Yar suggests that suitable targets comprise of online users who connect to the computer without safeguards or enough computer safety.\textsuperscript{336}

The second theoretical construct grounded in the Routine Activity theory is that cyberstalkers are motivated offenders who are determined to engage in cyberstalking offending. The second theoretical construct reflects Cohen and Felson’s suggestion that motivated offenders have the propensity and capability to commit crimes.\textsuperscript{337}

\textsuperscript{332} ibid
\textsuperscript{333} Kyung-Schick Choi ‘Computer crime victimization and integrated theory: An empirical assessment’ (2008) 2 International Journal of Cyber Criminology 1
\textsuperscript{334} The study was based on a self-report survey which contained multiple measures of computer security, online lifestyles and computer-crime victimization. The self-report survey was administered to 204 students
\textsuperscript{335} Ngo and Paternoster assert that the routine activities theory was postulated after the lifestyle exposure theory and merely incorporates the additional factors of motivated offended and capable guardian in addition to the element of a suitable target
\textsuperscript{336} Majid Yar ‘The Novelty of Cybercrime An assessment in Light of Routine Activity Theory’ (2005) 2 European Journal of Criminology 4
\textsuperscript{337} Lawrence Cohen and Marcus Felson ‘Social Changes and Crime Rate Trends: A Routine Activity Approach.’ (1979) 44 American Sociological Review 4
The third theoretical construct, which can be used to explain cyberstalking victimisation is that the absence of capable guardians enables cyberstalkers to access and target victims. Specifically, computer based capable guardians consist of anti-virus programmes, anti-spyware programmes, firewall programmes and other cyber security programmes that are manufactured to scan computer networks and files.\textsuperscript{338} However from a critical perspective, Holt and Bossler suggest that although protective software can assist in the reduction of risks, the measures cannot eliminate the likelihood of victimisation.\textsuperscript{339}

From a twofold perspective, the Routine Activity theory and the Lifestyle-Exposure theories have been applied to computer-crime victimisation with a view to developing a computer-crime victimisation model. In doing so, Choi developed the principle of digital guardianship with regards to the routine activity theory.\textsuperscript{340} The significance of Choi’s study is that it found that the two factors of online activities and digital guardians will contribute to computer victimisation. Applying the findings of Choi’s study, the researcher argues that cyberstalking victimisation may be reduced if victims install digital guardians in the forms of antivirus programmes, antispyware programmes and firewall programmes and do not engage in a risky online lifestyle.

Choi further argues that a means of avoiding computer victimisation is by applying the targeting-hardening strategy of the Routine Activity theory in the forms of up-to-date and adequate computer security systems.\textsuperscript{341} Adopting the targeting-hardening

\textsuperscript{338} Thomas Holt and Adam Bossler ‘Examining the relationship between Routine Activities and Malware Infections’ (2013) 29 Journal of Contemporary Criminal Justice 4
\textsuperscript{339} ibid
\textsuperscript{340} Kyung-Schick Choi ‘Computer crime victimization and integrated theory: An empirical assessment’ 2008) 2 International Journal of Cyber Criminology 1
strategy may in reality, not be a viable option to avoid cyberstalking victimisation. This is due to the fact that cyberstalkers engage in actions such as the dissemination of obscene and threatening messages on numerous publicly accessible social media websites involving online communities which would make it difficult for victims to absolutely avoid victimisation. Against this backdrop, Hutchings and Hayes carried out an exploratory study involving 104 participants, 50 of whom reported to having received a phishing email. The study found that cyber security safeguards may not prevent victimisation if email filters specifically are utilised in blocking a large number of spam emails.\textsuperscript{342} This finding suggests that in some instances, computer victimisation can still occur after cyber security measures have been implemented.\textsuperscript{343}

From an analytical perspective, a significant element of the Routine Activity theory is the requirement for the target to be in close physical and temporal proximity with the offender to be known and recognised.\textsuperscript{344} Therefore, Holt and Bossler highlight that in cybercrime offences, there is no physical convergence in space and time of offenders and victims.\textsuperscript{345}

From a critical perspective, the theoretical elements of physical and temporal proximity may affect the applicability of the Routine Activity theory to cyberstalking victimisation given that cyberstalkers and victims do not interact in the same physical location because cyberstalking is a crime which does not involve face-to-face contact between

\textsuperscript{342} ibid
\textsuperscript{343} A significant finding of Hutchings and Hayes’s study is that potential victims who engage in increased levels of routine activities relating to computer use and internet banking use are more likely to be attacked by motivated offenders. Based on Hayes and Hutchings’s findings and with reference to cyberstalking specifically, it may be argued that individuals who utilize computers a lot, are more likely to be victimised by motivated cyberstalkers who are seeking suitable targets\textsuperscript{344} ibid
\textsuperscript{345} Marleen Kranebarg, Thomas Holt and Jean-Louis Van Gelder ‘Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap’ (2019) 40 Deviant Behaviour 1
victims and offenders. Consequently, Yar argues that the Routine Activity theory and other theories of crime and causation seem to be of limited use in an environment that goes against presuppositions about how the socio-interactional context of the routine activities is constructed.\textsuperscript{346} However, in contrast to Yar’s views, Kranebarg, Holt and Van Gelder argue that although there is no convergence in space and time of offenders and victims in cybercrime cases, previous research indicates that offenders and victims in the end, interact with one another for cybercrime to take place asynchronously.\textsuperscript{347}

From a critical perspective, Leukfeldt and Yar further highlight that the available studies that have been conducted so far on the Routine Activity theory and cybercrime victimisation are subject to various limitations such as the reliance on a limited sampling set, limited sample size and the focus on a single aspect of crime.\textsuperscript{348} Leukfeldt and Yar write from a standpoint which argues that given that cybercrime occurs in the virtual realm where there is no convergence in time and space, certain aspects of the theory cannot therefore, be used to explain cybercrime.

Considering the above criticisms, the challenge for criminologists seeking to utilise the Routine Activity theory to explain cyberstalking victimisation with reference to the theoretical tenets of a convergence in time and space of the offenders and victims is two-fold. The first challenge for criminologists is to establish that cyberstalkers and victims converge in virtual time and space resulting in victimisation. The second

\textsuperscript{346} Majid Yar ‘The Novelty of Cybercrime An assessment in Light of Routine Activity Theory’ (2005) 2 European Journal of Criminology 4
\textsuperscript{347} Marleen Kranebarg, Thomas Holt and Jean-Louis Van Gelder ‘Offending and Victimization in The Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap’ (2019) 40 Deviant Behaviour 1
\textsuperscript{348} Eric Leukfeldt and Majid Yar ‘Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis’ (2016) 37 Deviant Behaviour 3
challenge for criminologists is to modify the traditional theoretical aspect of the Routine Activity theory to encompass offences that occur in the cyber realm. Crucially, Eck and Clarke suggest that the Routine Activity theory can be varied to explain crimes in which the victim and the offender do not interact at the same physical location. Specifically, Eck and Clarke argue that an offender may be able to reach a target through a network if they are part of the same geographically separate network.\footnote{John Eck and Ronald Clarke ‘Classifying common police problems: A Routine Activity Approach’ in Martha Smith and Derek Cornish (eds)\textit{Situational Crime Prevention} (Criminal Justice Press 2006)}

From a theoretical reformatory perspective, Reyns highlights that the growth in remote internet based routine activities and a consequential increase in criminal activities has led to a transformation of the theory to crimes in which the offender and the victim do not converge in time and space.\footnote{‘Bradford Reyns ‘Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact offences’ (2013) 50 Journal of Research in Crime and Delinquency 2} Reyns therefore, suggests that although the Routine Activity theory was developed to explain offences involving direct contact between the offender and the victim, it can be used to explain crimes which occur at a distance.\footnote{Reyns based his suggestions on the results of a study which found that the routine activities of individuals such as online banking and online shopping can lead to identity theft victimization}

Applying the reasoning of Reyns and of Eck and Clarke respectively to the cyberstalking victimisation model, it can be argued that although cyberstalkers and cyberstalking victims do not occupy or interact within the same physical location or converge in space and time, the traditional tenets of the Routine Activity theory is observed via the communication of cyberstalkers and victims within a network.
Importantly, Holt, Fitzgerald, Bossler and others, applied the Routine Activity theory to examine the relationships between online behaviours, target suitability, and cyber and mobile phone–based bullying victimisation. The study found that three factors predict online bullying and phone bullying victimisation. The three factors are access to technology, online routine behaviours and the target suitability. The findings indicate that Routine Activity theory is a credible framework that may be applied to explain online bullying. Given that cyberstalking and cyberbullying are similar digital offences, from the Routine Activity theory conceptual perspective, the findings of Holt and others can be used to explain the relationship between cyberstalking and cyberstalking victimisation.

2.4.5 Cyberlifestyle–Routine Activities Theory: Theoretical application to cyberstalking victimisation

The Lifestyle Exposure theory and the routine activities theory have been implicitly combined to posit a theoretical perspective referred to as the Lifestyle-Routine Activities theory. The theory postulates that the daily routines and behaviour of individuals can expose them to the risk of victimisation by criminals. Given the

---

352 Thomas Holt, Sarah Fitzgerald, Adam Bossler, Grace Chee and Esther Ng ‘Assessing the Risk Factors of Cyber and Mobile Phone Bullying Victimization in a Nationally Representative Sample of Singapore Youth’ (2014) 60 International Journal of Offender Therapy and Comparative Criminology 5
353 The study was based on a nationally representative sample of youths from nine schools across Singapore
354 Specifically, it can be argued that the three factors identified in the findings of Holt el, can equally contribute to cyberstalking victimization
355 Bradford Reynolds, Billy Henson and Bonnie Fisher ‘Applying the Cyberlifestyle Routines Activity Theory to cyberstalking victimization’ (2011) 38 Criminal Justice and Behaviour 1
academic debate on whether the Routine Activity theory can be applied to cybercrime because in the cyber environment, there is a divergence in time and space between the offender and the victim, the Cyberlifestyle-Routine Activities theory has been postulated. This iteration of the theory argues that the convergence of potential victims and offenders in time and space may not be the only necessary requirements to create an opportunity for victimisation within a cyber space environment.\textsuperscript{356} The theory was tested by Reyns, Henson and Fisher\textsuperscript{357} Their findings highlight that the predictors of cyberstalking victimisation are an increased exposure to motivated offenders, an increased proximity to motivated offenders, an increased online target attractiveness and online deviance. An additional significance of Reyns, Henson and Fisher’s study is that the findings suggest the risks for cyberstalking victimisation will be reduced if there is online guardianship to prevent against victimisation by disrupting criminal opportunity structures, thereby decreasing the likelihood of victimisation.\textsuperscript{358}

The importance of Reyns, Henson and Fisher’s study is that the authors utilised a modified Lifestyle-Routine Activities theory to empirically explain cyberstalking victimisation. In doing so, the authors expanded existing theories to victimisation in cyber space. However, the researcher did not apply the cyberlifestyle-routines activities theory to the current research because at the time of the study, the theory had not been sufficiently examined empirically with a view to establishing its applicability to cybercrime

\textsuperscript{356} ibid
\textsuperscript{357} Bradford Reyns, Billy Henson and Bonnie Fisher ‘Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending among college students’ (2010) 33 Deviant Behaviour 1
\textsuperscript{358} The theory examined the online routines and daily activities of individuals that may lead to cyberstalking victimization
In summary, there are two schools of thought that determine whether cyberstalking victimisation can be strictly viewed from the theoretical lens of the Routine Activity theory. The first school of thought holds that the theory cannot be applied to cyberstalking victimisation because cyberstalking is new crime which is committed in the new environment of cyber space. The second school of thought upholds Grabosky’s analogy of ‘old wine in a new bottle’ by arguing that cybercrime is simply an old offence in a new environment and can therefore be examined by application of the Routine Activity theory. The researcher identifies with the second school of thought and therefore applied to the coding of the data in this study, the three vital elements of the Routine Activity theory schema of a criminogenic environment namely motivated offender, suitable target and absence of a suitable guardian.

In conclusion, having reviewed the aforementioned seven theories, the researcher felt that the Routine Activity theoretical framework provided the best fit to the current study. The researcher chose this theoretical framework for two reasons. First, the theory has three distinct aspects which can be used to explain cyberstalking offending and victimisation. Second, the theory has been tested by different studies to explain cyberstalking victimisation. Consequently, the researcher analysed the interview date via the theoretical lens of the Routine Activity Theory in order to identify related coding.

2.5 The UK Cybercrime Strategies

Given that cyber criminals can take advantage of weaknesses in new technologies to threaten the safety of individuals, government, businesses and the economy, the UK government has introduced several measures to tackle cybercrime. Historically,
between 2009 and 2015, the UK introduced several strategies in a bid to tackle cybercrime in the UK with a view to protecting individuals, companies and the society at large. The strategies were superseded by the current National Cyber Security Strategy of 2016-2021. All the strategies are discussed in the sub-sections that follow:

2.5.1 The Digital Britain Strategy 2009

In March 2009, the government published the final report of the Digital Britain Strategy. From business and consumer perspectives, the report highlighted the need for the internet to be a secure means of communication. From a general perspective, the report highlighted the need for the internet to be safe to enable everyone to have confidence in utilising the internet for both business and pleasure. In doing so, the government recognised that giving everyone access to the internet raises safety and security issues which had to be addressed such as the prevention, detection, investigation and prosecution of cyber criminals.

2.5.2 The Cyber Crime Strategy and the Cyber Security Strategy: Aimed at protecting the UK in a digital world

Historically, one of the measures that has been introduced by the government to tackle cybercrime is the publication of the Cyber Crime Strategy by the Home Office in March

361 ibid
The aim of the Cyber Crime Strategy was to develop an amalgamated approach towards addressing the threats that have arisen with the development of the internet and associated technological devices. Specifically, the Home Office proposed to tackle cybercrime via this strategy by implementing five steps. The government’s strategy was subsequently updated as discussed in sub-section 2.5.3.

A second measure that was introduced by the government to tackle cybercrime was the publication of a UK Cyber Security Strategy titled ‘Protecting and Promoting the UK in a Digital world’. The strategy was significant because it highlighted that the government had established the office of Cyber Security Strategy in a bid to tackle cybercrime. The Cyber Security Strategy which was published on 25 November 2011 and highlights that the office was established to undertake two specific roles. The introduction of the office of Cyber Security Strategy indicates that the government is taking positive steps to enhance safe communication in the cyber realm. The governments’ commitment towards tackling cybercrime is further evidenced by its willingness to work with other government sectors and agencies to guarantee a coherent approach towards the tackling of cyber security threats. In the year 2015, the government indicated that it aims to achieve the vision of protecting individuals

---

363 ibid
364 The steps are intensifying government coordination to tackle cybercrime, establishing a hostile environment for cybercriminals, raising public confidence, working with the private sector and working international law enforcement officials
366 The office was established to undertake two specific roles. The first role is the provision of strategic guidance throughout the government. The second role is the development and harmonization of the UK Cyber Security Strategy
367 Some of the agencies include the National Cyber Crime Agency, the Police Central e-crime Unit, the Child Exploitation and Online Protection and Her Majesty’s’ Revenue and Customs
and businesses from cyber-attacks utilising the Cyber Security Strategy via four primary objectives.\textsuperscript{368}

In 2016, it was revealed that the 2011 National Cyber Security Strategy had delivered significant improvements to UK cyber security and achieved crucial results by investigating the market to steer secure cyber behaviours, the measure did not attain the range and rate of change necessary to out ride the fast moving threat.\textsuperscript{369} Consequently, the then Chancellor of the Exchequer announced that the UK government during the duration of the 2016-2021 subsequent National Cyber Security Strategy, will invest £1.9 billion into cyber security in a bid to achieve three cyber security aims.\textsuperscript{370} The aims of the National Cyber Security Strategy 2016-2012 as discussed in section 2.5.4, are defending systems and infrastructure, deterring adversaries, and developing societal capability ranging from companies individual citizens.\textsuperscript{371}

Given the above announcement, the researcher questions whether the 2011 Cyber Crime and Cyber Security Strategy highlighted above, assisted the government to counter cybercrime in general and cyberstalking specifically.

\textsuperscript{368} The first objective is to counter cybercrime and ensure that the UK is the most secure place globally to do business. The second objective is to enhance UK resilience to cyber-attacks and the third objective is for the UK to assist in creating a safe cyber space which can be used safely by the public. The fourth objective is for the UK to acquire the skill, knowledge and abilities that buttress the objectives of the cyber security strategy.


\textsuperscript{370} ibid

\textsuperscript{371} ibid
2.5.3 The UK Digital Strategy 2017

In March 2017, the government published the UK Digital Strategy 2017. The strategy has four primary aims. The aims are the growth of digital businesses, the trial of new technology and the promotion of advanced research. An additional aim is to ensure that every individual and every business acquires the skill and confidence required to embrace digital technology while having access to high quality internet.

The UK Digital Strategy 2017 has seven key strands which is envisaged will assist the government to fulfil specific goals. The first strand is the building of a world digital infrastructure for the UK to enhance connectivity or effective digital communication. This aspect of the strategy is geared towards ensuring that the UK can control heavy internet traffic. The second aspect of the strategy promotes the acquisition of relevant digital skills which will enable everyone to have digital access. The third aspect of the UK Digital Strategy 2017 is to ensure that the UK is the leading place to commence and grow a digital business. The fourth aspect of the strategy is geared towards assisting every British business to become a digital enterprise.

The fifth aspect of the UK Digital Strategy 2017, focuses on the promotion of a safe and secure cyber space with a view to ensuring that UK is the place globally to live and work in. This aspect of the strategy if successfully implemented will be crucial in preventing cybercrime victimisation given that measures will be introduced to tackle internet safety and security risks. The sixth aspect of the UK Digital Strategy 2017 is

---

373 ibid
374 This measure will assist hardware and software devices to communicate effectively with a range of other devices
375 The government anticipates that this will be achieved via a digital skills and inclusion process
376 This aspect of the strategy is based on a wider economy vision which is aimed at businesses
377 It is envisaged that this aspect of the strategy will be particularly effective in tackling cybercriminals
geared towards supporting the UK government as a global head in serving British nationals. The seventh and final aspect of the UK Digital Strategy 2017 is targeted towards improving public confidence in using data within the UK.

Given that the UK Digital Strategy 2017 is aimed at promoting a safe and secure cyberspace environment for UK businesses and citizens through the implementation of several measures, the researcher anticipates that certain aspects of the strategy may contribute to countering cybercrime in general and cyberstalking in particular by equipping UK citizens and businesses with the relevant digital skills that will promote cyber safety awareness and protect them from wide ranging victimisation online.

2.5.4 National Cyber Security Strategy 2016-2021

The strategy is a reflection of the governments’ decision to protect the UK economy and the privacy of citizens in a bid to secure UK technology from the ever growing threat of cyber-attacks. The government envisaged that the five year strategy will make the UK confident, capable and resilient in the fast-moving digital world by introducing stronger defences and promoting better cyber skills. Consequently, the government has invested £1.9 billion in defending the UK systems and infrastructure in a bid to deter cyber criminals who target businesses and individual citizens.

In light of the above, the researcher anticipates that the strategies that have been implemented by the government to equip companies and individuals with the skills that

---

379 Ibid
they require to defend themselves from cybercrime, might also educate individuals on how to protect themselves from cyberstalking victimisation given that cyberstalking is an aspect of cybercrime.

2.5.5 National Strategic Assessment of Serious and Organised Crime for 2018

The National Strategic Assessment of Serious and Organised Crime for 2018 (hereafter ‘NSA’), is an assessment based on intelligence which was introduced by the National Crime Agency. Significantly, the NSA on behalf of law enforcement identifies serious and organised crimes that are faced by the UK in order to coordinate responses to threats. The significance of the NSA in relation to cyberstalking as an aspect of cybercrime is that the assessment highlighted certain issues which may hinder the ability of law enforcement to act.

In summary, the various strategies highlighted above indicate that the UK government has taken positive steps to counter cybercrime from public, business and consumer perspectives. It is envisaged that certain aspects of the strategies will assist in tackling cyberstalking given that it is a type of cyber enabled crime.

2.6 Specialist UK Cybercrime Units

In the last decade, the UK government has created several units to assist law enforcement in countering cybercrime. The units all have the common aim of

---

381 In doing so, the NSA has identified cybercrime as one of the serious threats
strengthening the UK defences against cybercrime. Some of the units are discussed below.

### 2.6.1 National Crime Agency

The National Crime Agency is one of the agencies which has been created by the UK government to tackle cybercrime. The aim of the agency is to protect the public by tackling organised crime and bringing perpetrators to justice given that organised crime damages the lives of people and has a financial impact on the economy. The organised crimes range from cybercrime to the sexual exploitation of children.

Crucially, the National Crime Agency unit strengthens the UK borders, fights fraud and protects children and young people from sexual abuse and exploitation. In doing so, the unit works with several partners. Significantly, the agency has identified cybercrime as one of the organised crimes that poses a threat to the UK. The National Crime Agency has also, identified the theft of personal information in bulk from individuals, businesses or corporate networks for financial gain as an aspect of organised cybercrime which have been facilitated by the internet via online banking and e-commerce. Against this backdrop, it is arguable that as a hybrid of cybercrime, cyberstalkers may be investigated by officials of the National Crime Agency if the crime can be linked to offences that have been committed by online fraudsters for example who have targeted individuals, organisations and corporate networks for profit. This is more so because, the seven common cyber threats against consumers that have been

---

383 The common threats that UK faces from organized crime which have been identified by the national crime agency are child sexual exploitation and abuse, counterfeit currency, cybercrime, drugs, firearm, human trafficking, identity crime, intellectual property crime, kidnap and extortion, money laundering, organized theft, organized crime group and people smuggling
identified by the National Crime Agency are activities that can be engaged in by cyberstalkers.\textsuperscript{384}

2.6.2 National Cyber Crime Unit

The National Cyber Crime Unit is part of the National Crime Agency in the UK. The unit was created by the government to coordinate a response to the most serious cybercrime threats. The significance of the unit is that law enforcement officials in the unit have specialist capabilities which enable the unit to respond promptly to evolving cyber threats.\textsuperscript{385} In doing so, the unit works with other partners in a bid to tackle crime.\textsuperscript{386}

The National Cyber Crime Unit collaborates with partners to reduce crime by implementing four measures. The first measure is pursuing criminals on a national and international level via the provision of strong investigation responses to the most serious crimes. The second measures are adopting a proactive stance towards tackling criminal vulnerabilities and preventing criminal opportunities. The third measure that has been introduced by the National Cyber Crime Unit is helping the National Crime Agency to investigate cybercriminals. In doing so, the National Cyber Crime Unit offers technical support, intelligence support and training of the regional cybercrime units. The fourth measure adopted by the National Cyber Crime Unit through collaborating with other partners to reduce cybercrime is supporting partners

\textsuperscript{384} The highlighted common cyber threats against consumers are phishing, key logging, web cam manager, file hijacker, screenshot manager and ad clicker. The highlighted common cyber threats against businesses are hacking and distributed denial of service attacks

\textsuperscript{385} National Cyber Crime Unit (National Crime Agency) \texttt{<www.nationalcrimeagency.gov.uk/about-us/\_t>} accessed 15 December 2018

\textsuperscript{386} The partners include the Regional Organised Crime Units and the Metropolitan Police Cyber Crime Unit
within the law enforcement sectors to effectively protect themselves against cybercrime.\textsuperscript{387}

The researcher anticipates that the measures highlighted above will be utilised by police officers to tackle cyberstalking offending that is linked to organised crime such as hate speech, cyber terrorism, online sexual exploitation of children and online fraud for example. The National Cybercrime Unit offers training to law enforcement officials working in the specialist regional cybercrime units as opposed to all police officers and law enforcement professionals.

\textbf{2.7 Risk assessment of stalking victims}

The concept of risk has various aspects. The concept refers to identifying the nature of a threat, analysing the likelihood of the threat occurring and establishing the frequency of the threat with a view to either managing or eliminating the threat. Therefore Kropp, Hart and Lyon emphasize that the risk assessment of stalkers is difficult due to various factors ranging from the fact that stalking may encompass behaviors that are implicitly or indirectly threatening, and that the crime can be perpetrated over a long period of time.\textsuperscript{388}

Rosenberg highlights various risk factors that are unique to stalking which include a prior relationship between the stalker and the offender, substance abuse, mental

\textsuperscript{387} ibid
\textsuperscript{388} Randall Kropp, Stephen Hart and David Lyon. ‘Risk Assessment of Stalkers: Some Problems and Possible Solutions’ (2002) 29 Criminal Justice Behaviour 5

Rosenberg further argues that the fear of violence is one of the primary concerns experienced by stalking victims.\footnote{Ibid} McEwan, Pathe and Ogloff on the other hand, stress that the most effective way to measure and convey necessary information about individually relevant risk factors is by considering and analysing an individual’s personal history of violence or functional analysis of past behaviour.\footnote{Troy McEwan, Michele Pathe and James Ogloff ‘Troy Advances in Stalking Risk Assessment’ Behavioural Sciences and the Law (wileyonlinelibrary, 2011) <http://www.fixedthreat.com/perch/resources/mcewan-pathe-ogloff-2011-risk-assessment.pdf> accessed 19 April 2019}

Significantly, McEwan, Pathe and Ogloff indicate that stalking victims and stalkers themselves face four potential adverse outcomes ranging from the risk of physical violence towards the victim or a third party to the risk of psychosocial damage to the stalker.

It is arguable that the risk assessment of stalking and cyberstalking victims can enhance witness protection and facilitate the rehabilitation of offenders by ensuring that risks are identified, and interventions formulated to either manage or reduce the risk.

In the United Kingdom, some measures have been adopted by law enforcement and medical practitioners in the front line to risk assess stalking victims. To this effect, from a forensic psychiatric perspective, the specialist National Stalking Clinic was established in 2011.\footnote{The clinic is situated in Chase Farm hospital in Enfield North London.}


The private clinic is significant because psychiatrists at the clinic provide reports based on
the formal assessment of individuals who engage in stalking behaviour. The risk assessment reports provide suggestions on how identified risks can be managed. Additionally, the National Stalking Clinic provides assessments and consultation services regarding stalking circumstances in certain situations. Given that there is currently only one stalking clinic in the United Kingdom, the researcher anticipates that more clinics will be provided by the government in the future if it is financially viable for the government to do so. At the time of the study, additional stalking clinics had not been created to cater to stalkers and cyberstalkers implicitly.

As the primary prosecuting authority in England and Wales, the Crown Prosecution Service advises that prosecutors should when presented with a case either for charge or at court, ensure that police officers perform a full risk assessment. The CPS further recognizes that it is important that all the risks to a victim or the suspect are identified by the police or other agencies involved with the victim or suspect with a view to where possible, taking appropriate actions to reduce or remove such risks.

From an investigatory perspective, in 2009, the Association of Chief Police Officers introduced a risk identification assessment model for the offences of domestic violence, stalking and honour based violence (DASH). This measure was introduced to ensure that the police during the investigation process and other individuals who are in contact with the victim will implement measures to either identify or remove the risks. Consequently, as a result of the stalking law reform inquiry, twelve

---

394 The National Stalking Clinic receives referrals for risk assessment reports from various criminal justice agencies
396 By addressing the risk assessment of victims in the stalking and harassment guidance, the CPS demonstrates that the risk assessment of stalking victims is an important aspect of the investigation and prosecution processes
specific questions were incorporated in the DASH tool about stalking. The significance of the risk assessment tool with reference to stalking and cyberstalking implicitly, is that the tool has been designed in such a way which indicates that it is relevant to traditional stalking cases that involve perpetrators whose identities are known. This is evident in the fact that some of the questions on the stalking check list require victims to highlight how their safety is being threatened by a given stalking offender.

The DASH risk assessment tool was updated in 2016 and highlights that the four areas that trained front line officials are required to cover are; who is at risk, the context of the behaviour, how the risk factors interact with each other and the victim’s perception of risk. The problem with the DASH risk assessment tool is that some of the 12 risk assessment questions as provided in the checklist cannot be applied to cases where victims are being stalked anonymously by a cyberstalker. This is because in such cases, the victims may be unable to provide definite information about anonymous cyberstalkers. Therefore, the police officers may be unable to foresee the risks that might place victims in danger and may then, be unable to protect the victims from imminent or potential risks.

In 2011, the police introduced the Violent Crime Integrated Offender Management system to ensure that the police and other criminal agencies collectively monitor the most prolific offenders who cause harm in the community. Grimstead, highlights that

398 ‘Stalking and harassment screening questions -S-DASH’ (2012) <http://www.dashriskchecklist.co.uk/stalking> accessed 12 October 2018
stalking risk assessments are provided under the Violent Crime Integrated Offender Management. The risk assessments are be based on the S-Dash stalking risk assessment tool. Two additional risk assessment tools which are identified as part of the Violent Crime Integrated Offender Management are the Stalking Assessment Manual and the Stalking Risk Profile which provide police officers the opportunity to make informed decisions when risk assessing stalking victims. It is anticipated that the three stalking risk assessment tools highlighted above will assist police officers in gauging the dangers that stalking victims are in. Additionally, NPCC and CPS have developed a joint NPCC and CPS Checklist which is used by police forces and CPS in cases of Harassment or Stalking. The S-Dash stalking risk assessment tool and the joint NPCC and CPS Checklist – for Use by Police Forces and CPS in Cases of Harassment or Stalking are contained in Appendix 5.

It is arguable that the above highlighted tools will enable police officers to risk assess victims of stalking in the physical or cyber realm whose identities are known specifically as opposed to anonymous cyberstalkers. This is because as previously mentioned, some of the screening questions on the above highlighted risk assessment tools are only applicable to cases involving stalkers whose identities are known. The Stalking and Harassment Screen Questions (S-Dash) is contained in Appendix 5.

In 2015, the Home Office published the key principles of the Integrated Offender Model which is aimed at ensuring that criminal agencies work together to ensure that specific

401 ibid
persistent offenders receive the required support and are rehabilitated with a view to reducing offenders.402

2.7.1 The challenge of risk assessing cyberstalking victims: the issue of anonymity

From a preventative perspective, applying the concept of risk to the specific offending behaviour of cyberstalking may assist law enforcement and medical practitioners to develop the appropriate tools for risk assessing both cyberstalking victims and cyberstalkers. It is therefore important for law enforcement officials to adopt a dual approach to stalking risk assessment by firstly, risk assessing victims to ensure their safety and by secondly risk assessing perpetrators who have been engaging in cyberstalking behaviour with a view to managing the risks.

From a psychiatric disorder perspective, Mullen and others stress that stalking is a common social problem, often driven by psychiatric disorder in its perpetrators and productive of psychological and social damage in its victims.403 Mullen and others argue that the assessment and management of risk should indicate the following concerns of victims:

1. Whether the stalking will continue, or, if it has stopped, will it recur?
2. Whether the victim will suffer significant psychological and/or social damage,
which may include suicidal ideation or behaviour.

3. Whether the stalking will escalate to physical and/or sexual assault.\textsuperscript{404}

In theory, if the identity of the cyberstalker is known, law enforcement officials may be able to risk assess victims with a view to identifying potential risks and enhancing the safety of victims. The prompt and accurate risk assessment of cyberstalking victims may be a difficult task for police officers to accomplish if the cyberstalkers are anonymous. Consequently, police officers may be unable to assess and manage the risks of anonymous cyberstalkers to victims with a view to addressing the three areas of concerns highlighted above.

From an academic perspective with reference to stalking in the physical realm specifically, Kropp, Hart and Lyon argue that the risk assessment of stalkers is difficult due to a diversity of stalking-related behaviours.\textsuperscript{405} Applying this line of reasoning to the related behaviour to cyberstalking which can be perpetrated anonymously, it is plausible that it may be challenging for police officers to risk assess victims due to the varied nature of cyberstalking which is an aspect of the traditional crime of stalking in the physical realm.

Given that cyberstalking can lead to the deaths of victims, there is an onus on the ISPs to prevent perpetrators from harassing, threatening and intimidating victims online anonymously to ensure that police officers and prosecutors are able manage and

\textsuperscript{404} ibid
\textsuperscript{405} Prandall Kropp, Stephen Hart and David Lyon and Simon Fraser ‘Risk assessment of stalkers. Some problems and possible solutions’ (2002) 29 (5) Criminal Justice and Behaviour, p600
avoid risks more especially given that cyberstalking can escalate to stalking in the physical realm and vice versa.
Chapter 3  Methodology

This chapter describes the Methodology used to undertake the research for the thesis.

3.1 Rationale for the current research:

The research in this thesis sought to examine the perceptions of police officers and prosecutors on the law enforcement challenges that impede the investigation and prosecution of cyberstalkers in London. With this objective, the researcher discovered crucial issues perceived by the participants that frustrate them during the investigation and effective prosecution of cyberstalkers. The primary issues are difficulties in risk assessing victims due to staff shortages, the anonymity of cyberstalkers, lack of knowledge, victims refusing to support prosecutions due to a lack of confidence in the criminal justice system and lack of resources-manpower which result in heavy caseloads. The secondary issues are victim behaviour, evidential difficulties and lack of an effective specialist cyberstalking unit.

This research area was chosen because there is currently no joint research study on how both police officers and prosecutors in London perceive the investigative and prosecutorial challenges they face when dealing with cyberstalking offences.

The researcher applied Reyns research methodological approach to the study because it enabled her to recruit a sample of participants consisting of experienced law enforcement officials who provided relevant data. In doing so, the researcher moved beyond the conceptualisation of historically assumed common law enforcement difficulties which police officers and prosecutors encounter in the
investigation and prosecution of cyberstalkers to identification of the actual difficulties which police officers and prosecutors perceive hinder them from investigation and prosecution of cyberstalkers. The findings provide support for the identified recommendations.

### 3.1.1 Position of the Researcher in relation to the recruitment of her sample

It is noteworthy that the researcher was in the privileged position of being employed as a para legal officer by the Crown Prosecutor Service (CPS) which gave her access to prosecutors and police officers. The privileged position of the researcher enabled the researcher to hear first-hand accounts of participant views on the research topic. Further, given the law enforcement background of the researcher, her personal goal to research cyberstalking as an aspect of cybercrime influenced the researcher’s decision to choose this research area. Therefore, it has been acknowledged that it may be beneficial if a research study is influenced by personal goals and experiences. Strauss and Corbin argue that it may not be a limitation to choose a research problem through the professional route given that an individual researcher’s experience may be more important as a measure for the researcher to gauge whether a potential research endeavour will be successful.

As an employee of the CPS, the researcher recognised that her professional background may potentially lead to research bias during various stages of the research process. Simundic highlights that bias can occur in research either intentionally or unintentionally and can result in conclusions that are inaccurate and

---

406 Anslem Strauss and Juliet Corbin, Basics For Qualitative Research: Techniques for Developing Grounded Theory (2nd edn, Sage, 1988)
potentially misleading.\textsuperscript{407} Bias can lead to the distortion of truth and affect the reliability of findings. This is more so given that bias can occur at different stages of the research.\textsuperscript{408}

Crucially, bias can also lead to false conclusion and deviation from the truth.\textsuperscript{409} However, Smith and Noble argue that bias is present in all research and is difficult to eliminate.\textsuperscript{410} Specifically, Pannucci and Wilkins acknowledge that research bias can occur in planning, data collection and the analysis phase of research.\textsuperscript{411} Sica argues that a biased study can lose its validation in relation to the degree of the bias and acknowledges that it is impossible to eliminate bias.\textsuperscript{412} From an analytical perspective, Kilp suggests that bias in perceptions, behaviours and understanding refers to the extent to which evaluations lack an objective basis.\textsuperscript{413} Kilp therefore argues that there are various reasons for bias.

Given the above academic views on bias, the researcher recognised that research bias could occur during the selection and the interview stages of the research process.\textsuperscript{414} The researcher was particularly aware that given that she is a confident black, female professional who works alongside some of the participants, the issue of bias could prevent some of the participants from providing detailed responses due to a fear of losing their jobs. Additionally, the researcher was aware that due to the

\textsuperscript{407} Anna Maria Simundic ‘Bias in research’ (2013) 23 Biochem Med (Zagreb)
\textsuperscript{408} Joanna Smith and Hele Noble ‘Bias in research’ (BMI, 2014) 
<www.pdfs.semanticscholar.org/c49e/2f596d13b868421034ef9636caf925bbefcfd.pdf> accessed 21 January 2019
\textsuperscript{409} ibid
\textsuperscript{410} ibid
\textsuperscript{411} Anna Maria Simundic ‘Bias in research’ (2013) Biochem Med (Zagreb) 23 (1)
\textsuperscript{412} Christopher Pannucci and Edwin Wilkins ‘Identifying and Avoiding Bias in Research’ (NCBI, August 2010) <www.ncbi.nlm.nih.gov/pmc/articles/pmc2917235> accessed 21 January 2019
\textsuperscript{413} Gregory Sica ‘Bias in research Studies’ (2006) Radiology 238 (3)
\textsuperscript{414} Alair Kilp ‘The Positive and Negative Function of Perceptual Bia in Interpersonal Relations’ (Researchgate, 28 August 2017) <www.researchgate.net/publication/319256501> accessed 25 February 2019
\textsuperscript{414} The reasons range from to construct meanings to reducing the feelings of uncertainty

131
working relationship between her and the participants, the participants may be reluctant to fully divulge the issues that frustrate them in the investigation and prosecution of cyberstalkers due to a fear of possible disciplinary repercussions. Crucially, Vercruyssen, Wuyts and Loosveldt highlight that the characteristics of an interviewer can influence survey data collection processes. Vercruyssen, Wuyts and Loosveldt therefore suggest that the socio-demographic characteristics of interviewers can affect the probability of cooperation and the quality of the respondent’s responses.

Since the researcher has been employed within the criminal justice sector for over fifteen years, most of the different causes of bias highlighted above did not arise because the participants felt comfortable in the researcher’s presence and were therefore willing to give honest responses to the researcher’s questions. This was evident in their desire to take part in the study, answer questions in details, and provide additional responses when asked for clarifications and keenness to divulge additional information.

Nevertheless, the researcher acknowledges that it may be difficult for an outsider to gain access to closed professions such as the police force, armed forces and health services if the relevant gatekeepers are unwilling to act as middlemen between the researchers and the participants. Therefore, Clark acknowledges that the relationship between researcher and gatekeepers is crucial to gaining and maintaining access.

416 ibid
Gatekeepers are individuals, groups, and organisations that act as intermediaries between researchers and participants.\textsuperscript{417} Importantly, gatekeepers support the research process by providing an efficient and expedient conduit for access between researchers and participants.\textsuperscript{418} Clark argues that one of the reasons why gatekeepers may refuse to agree to a research request is if the research will lead to intrusion and the study is viewed as either as being critical towards a given gatekeeper or is in danger of exposing an area of practice that the gatekeeper does not want to be represented within the public domain.\textsuperscript{419} Clark further suggests that in such scenarios, it does not follow that such family or organisations in refusing research requests, have something to hide which ought to be revealed by the researcher but rather signifies that the gatekeepers face the danger of giving up control of how the researcher portrays their reality.\textsuperscript{420} Notably Holt, Bossler and Fitzgerald in explaining why there was a low response rate among specific law enforcement research participants, highlighted that participants may have had some reservations over proffering information on behalf of their organisations on matters relating to training and caseloads.\textsuperscript{421}

Okumus, Atinay and Roper emphasise that the difficulty of gaining access into organisations is one of the several issues that qualitative researchers encounter.\textsuperscript{422} Further, Okumus, Atinay and Roper note that it may be difficult to enter into an

\textsuperscript{417} Marlene De Laine ‘Fieldwork, Participation and Practice: Ethics and Dilemmas in Qualitative Research’ (Thousand Oaks 2000) 1
\textsuperscript{418} Tom Clark ‘Gaining and Maintaining Access Exploring the Mechanisms that Support and Challenge the Relationship between Gatekeepers and Researchers’ (2011) 10 Qualitative Social Work 4
\textsuperscript{419} Tom Clark ‘Gaining and Maintaining Access Exploring the Mechanisms that Support and Challenge the Relationship between Gatekeepers and Researchers’ (2011) 10 Qualitative Social Work 4
\textsuperscript{420} ibid
\textsuperscript{422} Fevzi Okumus, Levent Altinay and Angela Roper ‘Gaining access for research: Reflections from Experience’ (2007) 34 Annals of Tourism Research 1
organisation if the research is based on a sensitive topic.\textsuperscript{423} Importantly, Sleath and Bull stress that it may be difficult to recruit meaningful samples of police officers especially if the research topic is sensitive.\textsuperscript{424} Additionally, Sixsmith, Boneham and Goldring argue that there are inherent difficulties in gaining access to community research participants specifically.\textsuperscript{425}

Given that the police force like the armed forces is a closed profession, the researcher acknowledges that the police officers who took part in this study may have been reluctant or unwilling to be interviewed if she was not an insider who is currently employed within the CPS law enforcement sector.

Sampling bias is a type of bias which occurs when members of a selected population are less likely to be recruited than others.\textsuperscript{426} Sample bias occurs if the segment of respondents interviewed do not represent the group of interest thereby resulting in the interviewer interviewing the wrong people.\textsuperscript{427} Ngongo, Frick, Hightower and others highlight that sample bias can occur if research protocols are not observed thereby impeding the prospects of obtaining reliable survey data with regards to different interviewers interviewing a given population.\textsuperscript{428} In doing so, Ngongo, Frick, Hightower and others acknowledge that differences in gender, personality and familiarity can result in systematic bias. In addition to the above, the questions of interviewers can be

\textsuperscript{423} ibid
\textsuperscript{424} Emma Sleath and Ray Bull ‘Comparing Rape Victim And Perpetrator Blaming In A Police Officer Sample’ (2012) 39 Criminal Justice and Behaviour 5
\textsuperscript{425} Judith Sixsmith, Margaret Boneham and John Goldring (2003) ‘Accessing the Community: Gaining Insider Perspectives From the Outside’ 13 Qualitative Health Research 4
\texttt{<http://www.journals.plos.org/plosone/article?id=10.1371/journal.pone.0118025>} accessed 11 March 2019
\textsuperscript{427} ibid
\textsuperscript{428} ibid
biased if they influence the answers of the respondents given that the interviewers are in control of the question.

Given the above, the researcher adopted several measures in a bid to eliminate bias. The first measure that was adopted by the researcher to eliminate research bias was to recruit participants from different CPS and MPS offices to ensure that participants who had never worked with the researcher were recruited for the study. This measure enabled the researcher to recruit participants who had diverse views based on their varied experiences of working in different departments of the CPS and the MPS respectively. Therefore, when the study population was identified, the researcher used the same criteria to recruit the participants which involved, recruiting participants who had been employed as police officers or Prosecutors for over one year who had the experience of prosecuting defendants in different departments of the CPS and the MPS.

The second measure which the researcher adopted to eliminate research bias was to adopt a rigorous procedure. She achieved this through asking the participants standardized questions and using a consistent method for recording, analysing and interpreting the research data. In doing so, the researcher adopted the constant comparison analytical process which enabled her to analyse data in order to develop a grounded theory.

The third measure which the researcher implemented to avoid bias is asking general questions before specific questions during the interview so as not to influence the outcome of the participant answers. Additionally, the researcher adopted a fourth
measure to reduce bias which was to build a rapport with the interviewees in a bid to obtain honest and open responses. This approach enabled the researcher to summarize the responses of the participants at the end of the interviews and then question them to determine if the information that had been written down by the researcher was accurate.

This measure also enabled the researcher to analyse the data with an open mind and to challenge her assumptions. The fifth measure which the researcher adopted to prevent her own bias was to have an open mind during the data analysis and interpretation processes and to consider alternative causal explanations to the research findings as opposed to being overconfident in her own judgement.

The sixth measure that the researcher implemented was to screen and recruit prosecutors and police officers who represent the law enforcement officials that are responsible for investigating and prosecutors in London. The researcher did so by recruiting various experienced participants who work in the different departments of the CPS and the Metropolitan Police Service who investigate and prosecute cyberstalkers. The measures enabled the researcher to prevent confirmation bias by recruiting participants from diverse backgrounds treating all data equally. The seventh measure that the researcher implemented to prevent biased question was to write and ask neutral questions. Further, the researcher avoided asking the participants leading questions which infer the answers.

The researcher implemented the above measures to avoid deviation from the truth and to ensure that the study was credible given that some of the participants were her
colleagues. To this effect, Bogdan and Taylor highlight that a researcher may be able to recruit participants in the course of her daily activities.\textsuperscript{429}

Given that at the time of the study, the specific job roles of specialist cyberstalking Prosecutors or police officers had not been created at the CPS and the MPS, the researcher selected a sample of experienced prosecutors and police officers in a bid to obtain several points of view. This strategy resulted in the participants expressing divergent opinions and experiences which collectively provided an insight into the phenomenon under investigation.

In addition to the above the researcher was aware that her role as an interviewer might result in an unequal power balance. To this effect, Haworth argues that the role of every participant in interviews is defined and controlled.\textsuperscript{430} Haworth writes from a perspective which suggests that in police interviews, these roles are unequal in relation to the distribution of power and control.\textsuperscript{431} Consequently, in conducting the interviews, the researcher was aware that as an experienced employee of the CPS who has been employed for fifteen years given her institutional status, her role as an interviewer may be perceived as controlling. To maintain the balance of power and control between herself as the interviewer and the participants, the researcher implemented certain strategies to ensure that the participants disclosed information without challenging the interviewer. The strategies are establishing a rapport with the participants, listening attentively to their responses, being empathetic, seeking

\textsuperscript{429} Robert Bogdan and Steven Taylor, Introduction to Qualitative Research Methods (1\textsuperscript{st} edn, John Wiley & sons, 1975) 103
\textsuperscript{431} Haworth therefore argues that by controlling the setting of the interviews and having the ability to make decisions about the interviewee’s freedom based on the outcome, the police exert power over the interviewee. Further, Haworth suggests that the interviewees however have control over what they say. Additionally, Haworth asserts that the outcome of the interview is determined by the interviewee suspect despite the fact that the police is in control of the situation.
clarifications in a sensitive manner and not being judgmental. The strategies were significant because, given that the participants had institutional status too as investigative and prosecutorial law enforcement officials, there was a risk that the dynamics of the discourse could have been affected by their institutional roles and relative knowledge on the research topic.

Against the above backdrop, Haworth argues that factors such as the institutional roles of participants, the discursive roles assigned to them and their relative knowledge are factors which can affect the dynamics of power and resistance in a discourse.432

The researcher interviewed the participants to obtain the required data. In doing so, the researcher was conscious of the fact that personal traits can influence the data collection process. 433 To this effect, Vecrussyen, Wuyts and Loosveldt investigated the consequences of mismatching interviewers and sample units in relation to age, gender and education level on non-responsive indicators in Belgian data. Significantly, Vecrussyen, Wuyts and Loosveldt found that sample units participate more if the interviewer is more like them in age and gender. Similarly, Manderson, Bennett and Andadjani-Sutjahjo explored the social dynamics of interviews in respect of age, gender and class based on a sample of 50 participants with locomotor impairments.434 Manderson, Bennett and Andadjani-Sutjahjo concluded that factors such as age, gender and socioeconomic status can shape interviews and produce knowledge.435

434 Lenore Manderson, Elizabeth Bennett and Sari Andadjani-Sutjahjo ‘The Social Dynamics of the Interview: Age, Class and Gender’ (2006) 16 Qualitative Health Research 10
435 Manderson, Bennett and Andadjani-Sutjahjo found that the social relationship established during an interview is fundamental in multiple interview interactions
Manderson, Bennett and Andadjani-Sutjahjo also found that the interviewer would be in a privileged position if his or her workplace was used for the study. This is of interest in the current study as the researcher interviewed some of the participants at her workplace because they were her colleagues. Additionally, to ensure that certain participants were relaxed, the researcher interviewed some participants in public venues such as a coffee shop, a juice bar and cafes as requested by the interviewee. As previously discussed of, the researcher implemented several measures to avoid her privileged position leading to research bias.

3.1.2 Aims and objectives of the current research

The research in this thesis aims to examine the prosecution of cyberstalkers in the UK. The research relies on the experiences and perceptions of London prosecutors and police officers.

The main objective of the research is to identify the factors that police officers and prosecutors feel prevent them from investigating and prosecuting cyberstalkers. In so doing, the study will seek to explore the following:

(a) The extent to which perceived lack of knowledge impacts on the prosecution of cyberstalkers and the measures that are taken by police officers to acquire the knowledge they lack
(b) How the issues of anonymity and lack of resources might affect the effective risk assessment of victims of cyberstalkers
(c) The impact of perceived lack of resources on the investigation and prosecution of cyberstalkers
3.1.3 Research Questions

In order to meet these aims and objectives the following research questions were investigated:

(1) What are the perceptions of police officers and prosecutors on cyberstalking and the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking?

(2) What factors do police officers and prosecutors perceive could frustrate them in the investigation and prosecution of cyberstalkers?

(3) What challenges do police officers perceive impede the risk assessment of cyberstalking victims?

(4) Do police officers and prosecutors perceive evidential challenges lack of resources and lack of training as presenting law enforcement difficulties?

3.2 The researcher’s theoretical worldview

The epistemological, assumption which was at the core of the researcher’s study is that the most effective way to understand a phenomenon is to recognize that there is no single unitary reality apart from our perceptions given that each individual has a point of view and experiences a different reality. This epistemological assumption recognizes that multiple realities exist.\(^436\)

\(^{436}\) Steven Krauss, ‘The Qualitative Research Paradigm And Meaning: Making A Primer’ (2005) 14 The Qualitative Report 10
Given the epistemological aspect of a theoretical perspective relates to learning about the world based on a paradigm, Ritchie, Lewis, Nicholls and others suggest that epistemology has two aspects. The first aspect concerns how people can learn about reality and the second aspect examines what constitutes the basis of knowledge. In effect, an epistemological issue refers to what is or what should be regarded as acceptable knowledge in a discipline. Bryman argues that research can be affected by several epistemological positions.

The researcher explored epistemological considerations in examining certain theoretical philosophical ideas. Specifically, the researcher applied the qualitative approach in contrast to the post-positivist approach because it is reliant on the historical and social perspectives of the participants as opposed to facts obtained from scientific experiments. The researcher’s theoretical underpinning was therefore of a qualitative dimension rather than that of a positivistic quantitative dimension because the qualitative assumption of the world is based on subjective interpretations as opposed to the quantitative principle of objective reality. Furthermore, if the researcher had applied the positivistic approach to the study, her role as a researcher would have been restricted to the collection of data and the interpretation of the data via an objective approach. In effect, applying the post-positivist approach would have entailed the researcher taking on the role of an independent observer as opposed to a researcher who is engaged with the participants in the research process.

437 Jane Ritchie, Jane Lewis, Carol Nicholls and Rachel Ormston, Qualitative Research Practice (2nd edn, Sage, 2014) 6
439 Robert Bogdan and Steven Taylor, Introduction to Qualitative Research Methods (1st edn John Wiley & sons, 1975) 1
Therefore, Bogdan and Taylor emphasise that we lose sight of the subjective nature of human beings when we reduce them to statistical aggregates.  

3.3 Interpretivism

In addition to the above, the researcher examined the interpretivist epistemology to establish if it was an effective method to apply in the collection, analysis and interpretation of data. Interpretivism is a word attributed to a divergent epistemology to positivism. Bryman argues that interpretivism requires social scientists to embrace the subjective meaning of the social world as opposed to the application of a scientific model to the study of the social world.

Based on the above analysis in relation to interpretivism and constructivism, the researcher concurs with Ritchie and her colleagues on the following points:

1. Understanding the social world of people being studied and focusing on their meanings and interpretations produces knowledge
2. Meanings and interpretations based on the participants views can be constructed by researchers
3. The research process is essentially inductive because the interpretation is based on the data
4. Given that there are different perceptions and understandings, social reality cannot be captured accurately

440 ibid
442 Jane Ritchie, Jane Nicholls, Carol Lewis and Rachel Ormston Qualitative Research Practice (2nd edn Sage, 2014) 12
3.4 Qualitative methods

A significant feature of qualitative research is that it emphasises the significance of conducting the study from the perspective of the participants. An important feature of the qualitative research approach is the investigation of a phenomenon from the subjective viewpoints of the participants. William emphasises that qualitative research involves explaining, describing and interpreting data that has been collected. Therefore, in conducting this study, the researcher sought prosecutors and police officers who were willing to express their feelings by giving descriptive accounts of their views in relation to the cyberstalking phenomenon. The outcome was that the researcher described her findings from the subjective viewpoints of the participants.

Another reason why the researcher chose the qualitative method is because it enabled her to have direct contact and get close to the participants during the study. Patton suggests that the dual features of personal contact and insight constitutes the basis on which a researcher can gain an understanding of a phenomenon.

The researcher employed the qualitative approach to explore the meanings that certain individual prosecutors and police officers attribute to the phenomenon of cyberstalking from the perspective of law enforcement challenges. The qualitative approach afforded the researcher the opportunity to ask participants broad questions and to collate their comprehensive data based on their verbal accounts.

---

443 Evelyn Jacob, ‘Clarifying Qualitative Research: A Focus on Traditions’ (1998) 17 (1) Educational Research 16
445 Michael Patton, The Qualitative and Evaluation Research Methods (2nd edn Sage, 1990) 40
There are five aspects of qualitative research which include case study, ethnography, phenomenological study, grounded theory and content analysis. Hancock, Ockford and Windridge argue that the aim of a qualitative research is to develop explanations of social phenomena. Notably, the researcher applied the phenomenological aspect of qualitative research with a view to developing an explanation on the topic under investigation.

### 3.5 Phenomenology

Phenomenology is a qualitative methodological approach. The two features of phenomenology are that it studies the lived human experiences and the way things are perceived by individuals to the consciousness. Bogdan and Taylor argue that phenomenologists analyse the words of human behaviour as a means of gauging how people interpret the world. As a qualitative approach, phenomenology therefore allows interviewees the opportunity to give comprehensive views of the phenomena being researched.

From a historical perspective, phenomenological ideas can be traced to Edmund Husserl and Alfred Schutz. Bogden and Bilken suggest that the subjective aspects of individual behaviours are highlighted by phenomenologists who seek to access the conceptual world of participants. Given that the words and actions of the participants are sources which indicate how people view their world, it has been suggested that a

---

446 Beverley Hancock, Elizabeth Ockleford and Kate Windridge, ‘An Introduction To Qualitative Research’ (NIHR,2009) <www.rds-yh.nihr.ac.uk> accessed 22 June 2016


448 Robert Bogdan and Saria Biklen, Qualitative Research For Education (1st edn Allyn and Bacon 1982) 31
A phenomenologist will endeavour to visualize things from an individual’s behaviour.\textsuperscript{449} This is more so given that human beings understand reality only in the form which it is perceived.

Crucially, the researcher chose phenomenology as a methodology because it ensured that the detailed descriptions given by the participants were grounded in their perspectives.\textsuperscript{450} The phenomenology study enabled the researcher to understand the reality of London prosecutors and police officers who are responsible for investigating and prosecuting cyberstalkers.\textsuperscript{451}

Additionally, the researcher applied the Interpretative Phenomenological Analysis (IPA) based on which, the researcher identified emergent themes from the data, coded the emergent themes and analysed the experiences of the participants as evidenced in the numerous interview transcripts. To this effect, IPA has been specifically identified as an aspect of phenomenology which recognizes the dialogue between the researcher and the participants based on which the subjective viewpoints of the participants will be construed.\textsuperscript{452} Hancock, Ockleford and Windridge, stress that this approach recognizes that in attempting to analyse the experiences of the participants, the researcher will be required to interpret the accounts of the participants and then code the data for emergent themes.

\textsuperscript{449} Robert Bogdan and Steven. Taylor, Introduction to Qualitative Research Methods (1st edn John & Wiley, 1975) 14
\textsuperscript{450} Jane Ritchie, Jane Lewis, Carol Nicholls and Rachel Ormston Qualitative Research Practice (2nd edn Sage 2014) 3
\textsuperscript{451} Suffice it to say that the phenomenological approach enabled the researcher to comprehend and gain an insight into the cyberstalking phenomenon from the law enforcement perspective of the participants
\textsuperscript{452} Beverley Hancock, Elizabeth Ockleford and Kate Windridge, An Introduction to Qualitative Research (Research Design Service,2009) <https://www.rds-yh.mhr.ac.uk> accessed 22 June 2016
Specifically, the researcher applied IPA as a qualitative method to understand the subjective realities of the professionals through personal interpretations of their lived experiences and the meanings they attach to the experiences. Smith and Osborn suggest that the aim of IPA is to explain in detail how participants are making sense of their personal and social world.\textsuperscript{453}

Additionally, Smith and Osborn assert that the IPA approach is phenomenological given that it entails the detailed examination of a person’s lifeworld, endeavours to analyse an individual’s personal experience and is focused on an individual’s personal perception of an object or an event. Larkin, Watts and Clifton suggest that researchers should be amenable to adapting their views and be responsive to interpretation of data which is based on the responses of the participants.\textsuperscript{454}

Considering the above, IPA enabled the researcher to explore the lived experiences of the professionals and to develop an interpretative analysis of their experiences within social and law enforcement contexts. Significantly, the IPA enabled the researcher to understand that the experiences of the participants are within the specific research context in respect of the phenomena being investigated. Further, the IPA enabled the researcher to describe the perceptions of the professionals on cyberstalking victimisation and the threshold of acceptable behaviour on the internet.

\textsuperscript{453} Jonathan Smith and Mike Osborn ‘Interpretative Phenomenological Analysis (Research sites, 2012) < www://med-fom-familymed-research.sites.olt.ubc.ca/files/2012/03/IPA_Smith_Osborne21632.pdf> 1 March 2019

\textsuperscript{454} Michael Larkin, Simon Watts and Elizabeth Clifton ‘Giving Voice and Making Sense in Interpretative Phenomenological Analysis’ (2006) 3 Qualitative Research in Psychology 2
3.6 Research Methods

The researcher used two types of exploratory research methods to gather background data on the research topic.

3.6.1. Interviews

The first type of exploratory research design utilised by the researcher was in depth one to one qualitative interviews with a sample of the CPS and MET officials. Qualitative interviews are a vital research method for gauging or analysing the values or attitudes of individuals. Seale suggests that participants provide a better response to open ended questions and flexible questions in comparison to closed questions. In respect of the research study, the interviews enabled the researcher to gain an insight into the law enforcement challenges that are faced by prosecutors and police officers in the prosecution of cyberstalkers. The interviews also afforded the researcher the flexibility of encouraging the elaboration of issues.

The researcher utilised interviews as a qualitative research technique because it afforded her the opportunity to conduct detailed interviews with the limited sample size with a view to exploring their perspectives on the phenomena under investigation. In doing so, the researcher was given the opportunity to collect detailed data on the research questions. Additionally, the interviews ensured that the researcher was able to directly control the interview process with a view to seeking clarification of certain issues during the interview process if required.

455 Clive Seale, Researching Society and Culture (1st edition Sage, 2014) 209
The researcher relied principally on the verbal accounts with a view to obtaining data on the phenomenon under investigation and utilised open-ended questions to access the views of participants. In particular, the researcher used semi-structured interviews which lasted between 1 to 2 hours approximately. In conducting the interviews, the researcher ensured that the duration of the interview was adequate to address the issues that were raised on the one hand and that both she and the participants were not tired at any given point of the interviews.456

During the interview, the participants gave descriptive accounts of their opinions and an insight into the real challenges faced by London prosecutors and police officers in the prosecution of cyberstalkers. The first phase of the researcher’s interviews involved the researcher interviewing 25 experienced police officers, a Member of Parliament and a government adviser who were knowledgeable on the phenomenon being investigated. The second phase of the researcher’s interview involved the researcher interviewing 30 London prosecutors. The narrative of the police officers and the prosecutors provided further information on the phenomenon being investigated. Collectively, the interviewees confirmed the difficulties the prosecutors and police officers face in the prosecution of cyberstalkers.

The researcher collected data from one respondent at a time. The interviews were all transcribed and produced a lot of data. The researcher analysed the data with a view to identifying emergent and common themes. The researcher stopped interviewing when she reached theoretical saturation. Given the number of interviews, a lot of

---

456 Robert Bogdan and Steven Taylor, Introduction to Qualitative Research Methods (1st edn John & Wiley, 1975) 109
Qualitative data was produced which required interpretation and the researcher struggled to maintain an objective approach about the result and sought to prevent any preconceived idea from influencing the interpretation by staying focused on the research data.

In addition to the above, the researcher considered the findings of the Echo Pilot Survey on the analysis of cyberstalking in the United Kingdom prior to establishing the rationale for her research. The survey highlighted the impact of cyberstalking on victims from the perceptions of victims in addition to other points.

The issues of the regulation of cyberstalking and cyberstalking victimisation shaped the researcher decision to choose the research topic. This more so because in May 2015, the coalition government subsequently launched an online consultation on stalking laws. The final report highlighted the need for law enforcement officials to tackle the offence. From a victimisation perspective, the researcher analysed the finding of Short, Guppy, Jacqui Hart and James Barnes.

The above literature search shaped the research questions that were devised by the researcher which examines how police officers and prosecutors as front-line law enforcement officials perceive cyberstalking and the challenges that hinders them from investigating and prosecuting cyberstalkers.

---

Additionally, the researcher considered the finding of Drebing and others study on cyberstalking in large sample of social media users.\(^{461}\) The additional findings of Henselr-Mcginniss on the effect of cyberstalking victimisation on the academic performance of victims and the resulting psychological effects provided further information. From a domestic violence perspective, the findings of Alexy, Burgess, Baker and Smoyak on the perceptions of cyberstalking among college students was also considered.\(^{462}\) The findings indicate that victims of cyberstalking are more likely to be targeted by former partners.

3. 6. 2.  Literature search (Secondary data analysis)

The second method of exploratory research design that the researcher used was the literature search which enabled the researcher to gather information from academic texts, online journals, news media and published statistics. The researcher conducted a literature search prior to conducting the interviews to formulate the grounds for the research and establish the basis for formulating her line of enquiry. In doing so, the researcher considered the issues which were highlighted by the UK government consultation report on stalking which commenced on 14 November 2011.\(^{463}\) The aim of the consultation report was to identify how best to tackle stalking and cyberstalking with a view to protecting victims.

\(^{461}\) Harald DreBing, Josef Bailer, Anne Anders, Henriette Wagnar and Christine Gallas, Cyberstalking in a large sample of social network users: Prevalence, characteristics and impact upon victims’ (2014) 17 CBSN 61


\(^{463}\) ‘Have Your Say on Stalking Laws’ (Government, 14 November 2011) < www.gov.uk/government/news/have-your-say-on-stalking-laws> accessed 14 November 2011
The findings of the Independent Parliamentary Enquiry into stalking law reforms which was published in 2012 was additionally analysed by the researcher.\textsuperscript{464} From a legislative perspective, the report provided an insight on the criminalisation of cyberstalking in the UK. The findings of the report were the basis of the researcher’s question on the perceptions of the participants on cyberstalking and the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking.

Additionally, the findings of the review on cyberstalking in the UK conducted by the National Centre of Cyberstalking Research, shaped the research questions which were devised by the researcher.\textsuperscript{465} From a subjective perspective, the study is significant because it provided findings on the impacts of cyberstalking on victims based on the subjective experiences of 353 participant victims.\textsuperscript{466} The findings of the study shaped the researcher’s questions designed to explore the factors perceived by police officers and prosecutors which frustrate them in the investigation and prosecution of cyberstalkers given the impact of cyberstalking on victims.

Furthermore, the researcher reviewed the UK risk identification assessment model for the offences of domestic violence, stalking and honour based violence which was introduced in 2009 by the Association of Chief Police Officers.\textsuperscript{467} The researcher also considered the twelve specific questions incorporated in the domestic violence, stalking and honour based violence tool about stalking as a result of the stalking law


\textsuperscript{466} Two hundred and forty of the victims were female and one hundred and nine were male

\textsuperscript{467} Domestic Abuse, Stalking and Harassment and Honour Based Violence (DASH, 2009) Risk Identification and Assessment and Management Model
reform inquiry. The DASH tool and the risk assessment tools were introduced to ensure that the police during the investigation process will risk assess victims and manage identified or potential risks.

Additionally, the researcher analysed two further risk assessment tools which are identified as part of the Violent Crime Integrated Offender Management. The additional tools are the Stalking Assessment Manual and the Stalking Risk Profile which provide police officers the opportunity to make informed decisions when risk assessing stalking victims. The researcher analysed specific risk assessment tools and reviewed relevant literature on the risk assessment of stalking victims in a bid to devise questions regarding the perceptions of police officers and prosecutors on the risk assessment of cyberstalking victims.

In addition to the above, the researcher reviewed three relevant policies of the Metropolitan Police Service and one relevant guideline of the Crown Prosecution Service. The policies are the protocol on the appropriate handling of stalking or harassment offences between the National Chief's Council and the Crown Prosecution Service, the Stalking and Harassment Checklist and the ACPO Practice Advice on Investigating Stalking and Harassment. The relevant guideline of the Crown Prosecution Service which was reviewed by the researcher is the guideline on the prosecution of cases involving social media which was published in 2014. The various MPS and CPS policies enabled the researcher to devise questions on the factors

---

468 ibid
which police officers and prosecutors perceive hinder them in the investigation and prosecution of cyberstalkers.

Prior to the researcher devising the research questions, the researcher also analysed the findings of five relevant cases as reported by the media during the early stages of the research. The first case which the researcher considered was the case of Nigel Harris who was jailed on 15 October 1999 for using the internet to continue to stalk a victim who was his former partner despite a court order which prevented him from doing so.\(^{470}\) The case was significant as it was reported by the media as the first case of internet stalking in the UK which had resulted in the stalker being imprisoned.\(^{471}\) The second case which the researcher considered was the case of Shane Webber who was jailed on 11 October 2011 on for sending explicit photos of his former partner to her family, friends and adult websites and secretly posting twelve graphic photos of her to four social networking sites.\(^{472}\) The case was important because the victim who was cyberstalked for approximately 3 years by her boyfriend became suicidal and subsequently aborted their unborn baby as a result of stress.\(^{473}\)

The third case that the researcher considered was the case of Martin Poulter who made 16,690 random telephone calls to victims and received a 30 months custodial sentence in September 2012.\(^{474}\) The case was significant because it revealed that sometimes cyberstalkers target victims via phone only.


\(^{471}\) Ibid


\(^{473}\) The victim was prescribed antidepressants, developed symptoms of obsessive This compulsive disorder, stopped eating at times and had to retake her university exams because the abuse affected her so badly

\(^{474}\) Francesca Shanahan, ‘Married pervert spent over £5,000 of his benefits making lewd late night phone calls to random women’ (The Daily mail, 25 September 2012) <www.dailymail.co.uk/news/article> accessed: 30/10/12
The fourth case is the case of Andrew Meldrum who was convicted on 30 May 2014 of stalking and cyberstalking implicitly. Andrew Meldrum was convicted for spying on 2 victims through his computer after installing sophisticated spyware on their computers. This case was crucial because it highlighted that cyberstalkers can target complete strangers.

The fifth case that the researcher considered was the case of Clifford Mills who murdered his former girlfriend on 3 February 2011 Lorna Smith after stalking her via Facebook, text messages and telephone calls. This case was significant because it indicated that cyberstalking can lead to the death of victims in domestic violence cases.

Collectively, the five cases highlighted above indicate that cyberstalkers can target former partners or complete strangers via computer and phones and that the impact of cyberstalking on victims can range from psychological effects to the loss of life. Notably, the cases shaped the researcher’s question on whether it was realistic to expect police officers investigating cyberstalking cases to eliminate and manage all risks that threaten the safety of victims given that victims range from former partners to complete strangers.

475 Nicola Fifelied ‘Cyberstalker bugged Women’s Computer s to Spy on Them in their Bedrooms’ (The Telegraph, 30 May 2014) <www.telegraph.co.uk/news/uknews/crime/10866262/Cyber-stalker-bugged-womens-computers-to-spy-on-them-in-their-bedrooms.html> accessed 2 February 2018

476 He was ordered by the judge to undergo two years of probation supervision and do 20 sessions of one-on-one specified activities. He was also, placed on the sex offenders register for ten years and must pay £2,100 in costs to the prosecution

The above literature consisting of policies, guidelines, research studies, reports and case studies enabled the researcher to devise the research questions regarding the factors that police officers and prosecutors perceive frustrate them in the investigation and prosecution of cyberstalkers, the challenges that police officers and prosecutors perceive impede the risk assessment of victims, the criminalisation of stalking in the UK and the proactive measures that are taken by police officers and prosecutors to tackle the issue of lack of knowledge.

The literature search influenced how the researcher devised the research questions. Crucially, the review revealed that cyberstalking can have a devastating impact on victims, that the regulation of cyberstalking has been a cause for public concern in the UK within this decade, that certain factors may affect the risk assessment of victims and that that it may be challenging for police officers and prosecutors to bring cyberstalkers to justice.

The researcher visited various libraries when conducting the literature search. In conducting the exploratory research, the researcher did not use the ethnography research tool because the study did not require a detailed observation of the research participants. Further, the researcher did not use focus groups which are another type of exploratory research because of time constraints. The focus group session would have provided an additional means of gathering data as opposed to individual interview sessions. The researcher did not use focus groups because she would have found it challenging to arrange for selected law enforcement officials to simultaneously attend focus group interview sessions given the demanding job roles of the participants. It would have been difficult to organise focus group sessions as most of
the participants were busy reviewing cases, prosecuting defendants at court and investigating crimes.

The researcher did not apply the causal research design which seeks to establish the cause-and-effect between variables because the design relies on experiments to determine cause and effect. This study did not require an experiment due to the nature of the research.

3.7. The PhD design

The research in this thesis used a qualitative approach. The scope of the research was determined by the accessibility of most of the research participants who are law enforcement officials. It was initially envisaged that the research will be based on a cross-jurisdictional study requiring the researcher to investigate the challenges faced by law enforcement officials in the UK, Ireland and the US in the prosecution of cross-jurisdictional cyberstalkers. However, three years into the study, the researcher narrowed the scope of the research because it became apparent that what the researcher set out to accomplish was clearly over ambitious for a single PhD. Consequently, the research study was confined to the UK jurisdiction given that most of the data was obtained from prosecutors and police officers based in the UK as opposed to international law enforcement officials. This change resulted in a narrower research scope which required the researcher to focus the study on the UK jurisdiction as opposed to the additional jurisdictions of Ireland and the US. In doing so, the research covered the three following areas:
1 How lack of resources and lack of staff training are perceived by police officers and prosecutors in London as difficulties which frustrate them in the investigation and prosecution of cyberstalkers

2 The proactive measures that are taken by police officers and prosecutors in London to acquire the knowledge which they perceive to be lacking in the investigation and prosecution of cyberstalkers

3 The investigative impediments to the risk assessment of victims of cyberstalking as perceived by police officers and prosecutors in London who comprised the research sample.

The various sources of research data are interviews, texts, web pages and reports. Westbrook acknowledges that interviews are a valuable qualitative method and source of research data.\textsuperscript{478} Westbrook suggests that the onus is on the researcher to choose between structured and unstructured interviews. Notably, Caron, Bloom and Bennie acknowledge that although there might be a loss of information due to the pre-determined focus of the semi-structured interview, it could however result in an investigation of the concepts and ideas which are deemed to be the most crucial aspects of the phenomenon under investigation.\textsuperscript{479}

Taking the above factors into consideration, the researcher chose one to one semi structured interviews which comprised of open-ended questions. The settings for the interviews were the various CPS offices, police stations, police buildings, Westminster parliament and a government building in Northern Ireland.

\textsuperscript{478} Lynn Westbrook, ‘Qualitative Research Methods: A Review of Major Stages, Data Analysis Techniques and Quality Controls’ (Deep blue, 1994) \textless www.deepblue.lib.umich.edu \textgreater accessed 17 May 2017

The researcher found the interviews an advantageous method for collecting data for two reasons. First, the interviews enabled the researcher to ask the participants precise questions connected to the phenomenon under investigation. Second, the interviews afforded the researcher the opportunity to probe the participants for details of their experiences and to seek clarifications on initial points that they had made. Various accounts emerged from the interviews which provided an insight into the phenomenon under investigation.

3.8 Sampling

Collingridge and Gantt suggest that there should be a clear rationale for selecting participants and that they should fulfil a specific purpose related to the research question. Given the purpose of the study, the rationale for the sample was to recruit participants who as primary law enforcement officials, can provide dense information on the phenomenon under study based upon their professional knowledge and personal experiences. To this effect, Cleary, Horsfall and Hayter highlight that the purpose of the inquiry among other factors will determine the make-up of the participants and numbers of participants. Further, Cleary, Horsfall and Hayter list the purposeful choosing of participants, the intense studying of small numbers and the identification of a rationale for the selection as some fundamental principles of participant selection and this approach felt relevant for the current research.

480 Dave Collingridge and Edwin Gantt ‘The Quality of Qualitative Research’ (2008) 23 American Journal of Qualitative Research 5
481 Michelle Cleary, Jan Horsfall and Mark Hayter ‘Data Collection and Sampling in Qualitative Research: Does Size Matter?’ (2014) 70 Journal of Advanced Nursing 3
Notably, the researcher applied Reynolds' research methodological approach to the study by recruiting a sample of participants who either had the experience or were experiencing the research topic under investigation as law enforcement officials who are in the frontline of bringing cyberstalkers to justice. This approach, therefore, enabled the research to obtain data from police officers and prosecutors who are in the field of investigating and prosecuting cyberstalkers and directly involved in bringing them to justice.

Specifically, the police officers have personal experiences of investigating cyberstalkers and the prosecutors have the experience of both charging cyberstalkers and reviewing cases on cyberstalking. Collectively, the sample chosen by the researcher provided dense and credible data which enabled the researcher to give an account of the phenomenon under investigation. On identifying the rationale for the study, the researcher selected the sample with a view to interviewing the participants in detail given their personal experiences in investigating and prosecuting cyberstalkers. In choosing the sample, the researcher envisaged that the participants would be able to provide rich data on the research questions which will enable the researcher to provide a persuasive account of the phenomenon of interest.

Purposive sampling is the most appropriate sampling method to employ in qualitative research. Maxwell emphasises that the significance of purposive sampling is that it can be used when a particular setting, individuals, or events have been selected due to the fact that they capture the diversity of a population. Based on Maxwell's line of reasoning, the researcher utilised the purposive sampling method to select a sample.

---

482 Joseph Maxwell, ‘Designing A Qualitative study’ In Leonard Bickman and Debra Rog (eds), The Sage Handbook of Applied Research Methods (Sage 2009)
of London prosecutors and police officers respectively because they could provide data on the cyberstalking phenomenon given that they are the primary law enforcement officials in the UK for prosecuting cyberstalkers.

Additionally, the researcher utilised the snowball sampling method which entails the researcher identifying the specific participants that have been interviewed to request further interviewees. Dragan and Isaic-Maniu argue that the primary benefit of the snowball sampling method is that it enables researchers to access segments of the hidden population that are not easily accessible. Applying this line of reasoning to her study, the researcher argues that utilising snowball sampling enabled her to further recruit participants within sections of the population. The snowball sampling method specifically enabled the researcher to recruit participants who were based at the Serious Organised Crime Agency, New Scotland Yard and the Police Central e-Crime Unit. The snowball sampling method also enabled the researcher to recruit prosecutors who were based in other CPS offices such as the Crown Court Unit, Fraud Unit, Serious Complex Casework Division, and the Rape and Serious Sexual Offences Units. This was facilitated by the fact that some of the participants who were interviewed by the researcher recommended other experienced participants who could contribute to the research study.

The researcher gained access to the further participants after she was given the names, telephone numbers, email addresses and office locations of specific police officers and prosecutors who it was felt could contribute meaningfully to the research.

---

given their specialist backgrounds. The researcher contacted the recommended participants to request interviews with them at a place and at a time that was convenient from them. The participants when contacted, expressed their willingness to take part in the study and confirmed the dates, the time and the locations of the interviews. Two factors contributed to the researcher gaining access to the specialist participants. The first factor is that the researcher is currently employed by the CPS and as such, the participants were not suspicious of her research motives. The second factor is that the study has been approved by the CPS and the MPS respectively and as such, the participants were aware that the researcher had legally obtained the permission of their respective employers to approach the participants for an interview.

Specifically, through snowball sampling, two police officers who were interviewed recommended that the researcher recruits senior police officers who were based at New Scotland Yard and the Police Central e-Crime Unit respectively because they would provide specialist insight on the research topic. In doing so, the police officers provided the names and contact details of the recommended participants following which, the researcher contacted the recommended participants to recruit them for the study. In a similar vein, during the interviews four prosecutors provided the details of specialist prosecutors in the Crown Court Unit, Fraud Unit, Serious Complex Casework Division, Fraud Unit and the Rape and Serious Sexual Offences Units.

The researcher was granted access to four additional prosecutors because some prosecutors whom she had previously interviewed, recommended the additional specialist prosecutors whose specialist experience was relevant to the study. As a result of her contacts within the CPS, the researcher was therefore, able to recruit
additional prosecutors who were willing to take part in the study. In doing so, the researcher travelled to the various offices to conduct the interviews. On initially contacting the participants via email, the researcher provided an overview of the research objectives and the researcher’s background. The researcher also followed this up dealing with the pre-interview queries that were raised by some of the participants to ensure that they were fully informed on the objectives of the study.

The researcher adjusted the makeup of her sample slightly because while interviewing, she became aware that a Member of Parliament who chaired the UK inquiry into stalking law reforms had just published his finding based on which the coalition government had subsequently agreed to create new legislation on stalking. Consequently, the researcher decided to recruit the Member of Parliament (MP) as a participant with a view to establishing whether his recommendation covered the criminalisation of cyberstalking specifically and the prosecution of cyberstalkers in general. The researcher recruited the Member of Parliament to ascertain whether his recommendations reflects the perceptions of the police officers and the prosecutors given that he is a policy maker. Crucially, the researcher’s aim in recruiting the Member of Parliament was to establish whether his recommendations reflect the reality of the police officers and the prosecutors who are the law enforcement officials in the forefront tasked with bringing cyberstalkers to justice.

In relation to social media providers, the Member of Parliament raised the issue of Facebook changing the privacy settings of customers without notifying them thereby enabling cyberstalkers to target customers. The Member of Parliament further raised the point that some members of the public enable cyberstalkers to target them by
putting pictures on Facebook and posting messages on Facebook without realizing that Facebook operates an open profile for all as opposed to a private profile. Consequently, the Member of Parliament argued that a combination of the open profile that is operated by Facebook and the changing of privacy settings by Facebook provides avenues for cyberstalkers to target victims. The Member of Parliament therefore stressed that this situation was particularly worrying given that children under the age of 13 can open accounts on Facebook despite the fact that they are under-aged. He therefore recommended that there should be an intensive public awareness programme and an education of the public on these issues.

In relation to the ISPs the Member of Parliament suggested that the ISPs should take more responsibility to monitor the information that customers provide when they sign up for an account. He therefore questioned why customers can sign up for internet accounts using fake details without thinking that they might be sued for libel.

Some of the above perceptions of the Member of Parliament on cyberstalking victimisation mirrors the perceptions of certain participants in relation to training, education and the responsibility of ISPs.

3.9 Access

On identifying the organisation where they would like to carry out research, several academics may encounter various impediments in attempting to gain access to several institutions. Satirenjit Johl and Sumathi Renganathan argue that organisations are often suspicious about the role of strangers.

In relation to the CPS given that the researcher is an employee of the organisation, the CPS management were very supportive of the researcher’s goals. Consequently, the organisation promptly approved the research and granted the researcher access to several London prosecutors. In addition, the organisation paid for the researcher to attend a relevant conference which was organised by the MPS.

In relation to the MPS, the organisation was initially sceptical about the researcher’s motives given that she is not employed by the organisation. However, after an official of the strategy and research policy department carried out enquiries which confirmed that the researcher was an employee of the CPS, the MPS formally gave their consent for the researcher to interview 30 police officers. Consequently, in June 2012, the official at the research and strategy department confirmed that the researcher did not require additional vetting because the researcher was an employee of the CPS. The official acted as the gatekeeper for the MPS in this regard by providing formal access to the police officers. This research privilege enabled the researcher to gain access to the interview police officers without being additionally vetted because she was employed by the CPS.

The researcher recognizes that another researcher who works outside the criminal justice system would not have been given formal access to the research participants without being additionally vetted. To this effect, Ray and Zaretsky highlight that researchers and educators are required to explore the concepts of privilege and bias
as part of doctoral training as professional experiences develop. Consequently, the researcher acknowledged the concept of research privilege by ensuring that she applied the principles of confidentiality, anonymity and voluntary consent when interviewing the participants and also ensured that measures were put in place to guard against bias in the research as previously described in detail in Section 3.1 of chapter 3.

3.9.1 Access to the prosecutor sample

Following receipt of approval by the CPS, their communications department notified all members of staff in London by sending out a general email. The email informed members of staff of the researcher’s topic and requested that all the prosecutors cooperate with the researcher to take part in the study. A senior CPS official acted as a gatekeeper for the CPS stakeholder in this regard by providing access to the prosecutors.

Gaining access to the research sites entailed the researcher travelling to various CPS offices to interview the prosecutors. Some of the offices that the researcher travelled to include the Serious Organised Crime department, the Rape and Serious Sexual Offences department, the Crown Court department and the Magistrates Court department which was formerly based in Croydon. Additionally, the researcher visited various crown courts such as Isleworth crown court, Inner London Crown Court and

---

Snaresbrook Crown Court to interview Higher Court Advocates who are prosecutors that have been given higher advocacy rights.

3.9.2 Access to the police officer sample

Subsequent to receiving approval from the MPS strategy and research department, the researcher interviewed experienced police officers who were based at Acton police station, the Serious Organised Crime Agency, New Scotland Yard and the Police Central e-Crime Unit. The MPS official acted as a gateway for the Metropolitan Police Service by providing access to the police officers.

3.9.3 Access to a Member of Parliament

A parliamentary research assistant provided access to a Member of Parliament who the researcher interviewed at Westminster parliament. The parliamentary research assistant acted as a gateway facilitating the interview.

3.9.4 Access to the ISPs

It was challenging to gain access to the ISPs because the researcher was unable to contact Google, Facebook or Twitter officials as at the time of the study, there were no apparent means of directly contacting the organisations via email or telephone. It would seem that the only measure that has been provided by ISPs is for customers to use the Help Centre for the sole purpose of reporting problems with their accounts. There were no identifiable gatekeepers for the ISPs. Although the study did not indicate the views of the ISP representatives, a lot of useful data was generated from the various interviews with other participants.
3.9.5 Recruitment of the prosecutors and police officers

A vital aspect of conducting qualitative research is recruiting participants for the study.\textsuperscript{486} Namageyo-Funa argues that it may be tasking for a researcher to choose the most appropriate recruitment method. In carrying out the study, the researcher chose to recruit prosecutors and police officers because they are the primary law enforcement officials in the UK for prosecuting cyberstalkers. In recruiting the participants, the researcher chose several methods which include face to face interactions, emails and telephone calls. In doing so, the researcher sent a covering email to some of the participants. The email provided information on the topic of the researcher’s study, her job role, the length of the proposed interview and confirmation that her study had been approved by the CPS management.

In attempting to recruit participants, the researcher also sent follow up emails to specific prosecutors whom she wanted to interview for the study based on their experience and availability.

As there was neither a specialist cyberstalking department in the CPS nor a specialist cyberstalking prosecutor at the time of the study, the researcher ensured that the prosecutors that she recruited represented a sample of the prosecutors based in the core CPS offices. The prosecutors worked in the Domestic Violence Unit, the Magistrates Court Unit, Rape and the Serious Organised Casework Crown Court Unit. The first, second and third prosecutors were senior crown prosecutors who specialized

\textsuperscript{486} Apophia.Namageyo-Funa, Rimando, Brace, Christiana, Fowles, Davies, Martinez and Sealy: ‘Recruitment in Qualitative Research: Lessons Learned During Dissertation Sample Recruitment’ (2014) 19 Qualitative Report 4
in domestic violence cases and rape and serious sexual assault cases and serious casework cases. They were responsible for reviewing cases, preparing cases for trial and liaising with police to ensure that the cases were robust evidentially. They were based in the crown court unit of the CPS. The fourth prosecutor had the managerial role of a Borough Crown Prosecutor. He was based in the magistrate’s court unit of the CPS and line managed some of the prosecutors.

The researcher's rationale for recruiting a varied sample of prosecutors is that given that the review of cyberstalking cases is not confined to one department, there was a strong likelihood that the participants would have some routine experience of prosecuting cyberstalkers in their everyday activities. The researchers applied the same rationale in recruiting police officers from various police departments.

In recruiting the prosecutors and the police officers, the researcher used three measures which include face to face recruitment of the prosecutors and police officers, recruitment via the recommendations of participants, recruitment via emails and recruitment via telephone calls. An important feature of the researcher's recruitment method was that her relationship with the participants was based on mutual trust and respect.

Bogdan and Taylor argue that researchers should not recruit colleagues as participants as the participants may only reflect the views that are beneficial to them. Therefore, the researcher acknowledges that given the sensitive nature of the data that was gathered from the study, the participants as high-ranking professionals may

---

487 Robert Bogdan and Steven Taylor, Introduction to Qualitative Research Methods (1st edn John Wiley & sons, 1975) 103
have felt their professionalism could be threatened by their honest revelations of the difficulties that they face in the investigation and prosecution of cyberstalkers. Nevertheless, their feelings of frustration were coupled with an anticipation that this research finding will in some way, lead to the implementation of suggested reforms. From this perspective, recruiting certain prosecutors who are the researcher’s colleagues was beneficial to the researcher’s study.

It should be reiterated that, significantly, the researcher was in the privileged position of being employed as a para legal officer by the CPS which gave her access to eight prosecutors who the researcher had previously worked with ten years prior to the research and twenty two other prosecutors who the researcher had never worked with. The eight prosecutors who the researcher had previously worked with included two higher court advocates who have higher right of audience in the crown court and six office based crown court prosecutors. The higher court advocates are responsible for drafting indictments, preparing cases for trials and presenting cases in court. The prosecutors are responsible for giving charging advice to police officers, liaising with police officers, reviewing case, drafting indictments and preparing cases for trials. The researcher previously worked with the eight prosecutors ten years ago in her capacity as a regional Direct Communications with Victims Co-ordinator which entailed her writing to victims and meeting victims and their families when charges had been dropped by the CPS.

The privileged position of the researcher enabled the researcher to hear first-hand accounts of participant views on the research topic. Further, given the law enforcement background of the researcher, her personal goal to research cyberstalking as an
aspect of cybercrime influenced the researcher’s decision to choose the research area.

As an employee of the CPS, the researcher recognizes that her professional background may lead to research bias during various stages of the research process. The issue has been dealt with earlier in Section 3.1.2.

The researcher encountered two problems when attempting to recruit prosecutors for the study. The first problem was that five out of the thirty prosecutors whom the researcher approached for an interview, did not respond to her emails. To overcome the challenge, the researcher used additional recruitment tools such as follow up emails, repeated telephone calls and follow up face to face conversations.

The second recruitment problem the researcher encountered was that although the participants whom she recruited gave verbal consents, when she subsequently sent them consent forms via emails to sign and date, only some of the participants submitted their completed forms. The lack of response could be attributed to the fact that due to the researcher’s professional relationship with the participants, the prosecutors were content to rely on the initial consents that they had all given. Additionally, the fact that the participants gave their consents via emails without explicitly signing the forms could be viewed as implied consent.

3.9.6 Recruitment of the UK Member of Parliament and Probation officials

As previously mentioned, the researcher recruited the Honourable Elfyn Llywd M.P. who was a senior Member of Parliament and his parliamentary assistant to take part
in the study. The researcher recruited the Member of Parliament for two reasons. First, he chaired the parliamentary inquiry into stalking law reforms in the UK and published his findings based on which the government enacted legislation to criminalise face to face stalking and implicitly cyberstalking. Second, in conducting the enquiry, he heard evidence from various UK law enforcement officials. The researcher elicited useful responses from the Member of Parliament who provided additional information on the topic under investigation based on the findings of his own inquiry.

In addition to the above, the researcher recruited the former chair of the National Probation Service to take part in the study. The researcher recruited the probation official because he was part of the inquiry which had reviewed the stalking legislation in the UK on behalf of the coalition government. The participant provided an insight into the phenomenon under investigation from the perspective of victims.

3.9.7 Interviews

The researcher used qualitative interviews to collect the relevant data for the study. In particular, the researcher used semi structured interviews. Qualitative and semi-structured interviewing share some common characteristics. The first characteristic is the holding of face to face dialogue with two or more participants. The second characteristic is that the interview methods are both based on selected themes the researcher has chosen to investigate via flexibly structured interviews. The third shared common characteristic between qualitative and semi-structured interviews is that there is an onus on the researcher to obtain knowledge based on the perspectives

---

488 Rosalind Edwards and Jane Holland, What is Qualitative Interviewing? (first edn Bloomsbury academic, 2013) 13
of the participants which need to be put in context. These three features were manifested in the researcher's interviews.

It is acknowledged that participants will be able to identify with academics and more willing to take part in a study if they are informed of the researcher’s motive. Consequently, prior to starting the interviews, the researcher informed the participants that her motive for embarking on the study was to present relevant findings for the benefit of the law enforcement officials and to add knowledge to this developing area of criminal law. On receiving the notification, the participants were keen to contribute to the study. The interview questions were prepared in advance and consisted of several open-ended questions. The questions can be found in Appendix 3.

3.9.8 Analysis of the data

The researcher adopted a two-staged process in the analysis of data. The approach enabled her to conduct a preliminary analysis and identify common themes at a very early stage of the study. Preliminary analysis of the data enabled the researcher to identify emergent themes and to ascertain the issues that require clarification via literature review. Consequently, the researcher conducted an analysis of the data in conjunction with the literature review.

The emergent themes which were identified are anonymous cyberstalkers, risk assessment of victims, risk assessment of cyberstalkers, lack of resources, lack of experts, proving cases, lack of training, lack of knowledge, evidential difficulties, under

489 ibid
490 Robert Bogdan and Steven Taylor, Introduction to Qualitative Research Methods (first edn John Wiley & sons, 1975) 105
reporting by victims, victims not cooperating in domestic violence cases, meeting the evidential threshold, ISP, delays, demanding caseloads, personal online responsibility, cyberstalking via unregistered SIM cards and mentally ill cyberstalkers. As previously mentioned in section 3.6.1, as part of the literature review, the researcher analysed the relevant MPS policies and CPS guidelines in addition the researcher examined the relevant academic texts, research studies journal articles and case law.

3.9.9 Coding

On analysing the data, the researcher employed the qualitative analysis strategies of coding.491 Braun and Clarke suggest that codes pinpoint the characteristics of the data which refer to the essential segments or elements of the raw data that can be evaluated in a significant method regarding the phenomenon of interest.

Coding connotes the process of analysing data.492 Coding is the principal categorizing strategy in qualitative research.493 The coding of data facilitates the identification of themes by looking for word repetitions, looking for key-words-in texts, reading unmarked texts, and cutting up and sorting the transcripts.494 The researcher applied the coding strategy to the data analysis process because it enabled her to ascertain the repeated words, common phrases and identical patterns of sentences in the data. A main goal of the coder is to establish repetitive patterns and their consistencies as

493 Joseph Maxwell, ‘Designing A Qualitative study’ in Leonard Bickman and Debra Rog (eds), The Sage Handbook of Applied Re Methods (Sage 2009)
evidenced in a given piece of data. Saldana highlights that coding is a cyclical process.495

Taking the above factors into consideration, the researcher applied thematic coding in analysing the qualitative data. The advantages of thematic coding are that it minimizes the quantity of data, ensures that the reduced data can be easily read and facilitates the usage of specific themes to establish concepts.496 In applying thematic coding, the researcher broke down the data contained in the interview transcripts into themes in a bid to identify underlying concepts.

In analysing the data, the researcher read the transcripts repeatedly with a view to understanding the data comprehensively. This approach enabled the researcher to identify and keep a record of the themes and categories of themes. On identifying the themes, the researcher highlighted the similar segments of the transcripts with a code label to enable the researcher to retrieve them subsequently for further comparison and analysis. The researcher based her coding on key words, themes, phrases and topics. The researcher created new codes on discovering that a theme identified from the data does not reflect the codes already identified. The advantage of the approach that the researcher took to coding the data is that it enabled the researcher to go through the data methodically and to identify the subject matter contained in the data.

The researcher used highlighters and post-it notes to distinguish the various concepts and categories. The researcher also noted the relevant codes in the margin next to

495 Johnny Saldana, The Coding Manual For Qualitative Research (3rd edn ,Sage 2001) 45
496 ibid
the relevant data in the hard copy of the transcripts. The open coding generated a long list of codes which the researcher classified into categories and via the use of spider diagrams. The list of codes are contained in Appendix 6.

On completing the open coding, the researcher applied the second stage of axial coding which is the process of exploring the relationship between the categories of identified data and their highlighted properties. The significance of axial coding is that it facilitates the construction of data that was previously categorized via open coding. This approach enabled the researcher to determine the relationship between the concepts and the categories.

On completing the axial coding process, the researcher embarked on the selective coding process which enabled the researcher to identify one category of codes as the primary category around which all other categories are based. In addition the Researcher applied three elements of the Routine Activity Theory (Cohen and Felson, 1979) (motivated offender, suitable targets and absence of a suitable guardian) to the codes in order to identify those codes that might relate to the theory, these codes are marked with an asterisk in Appendix 6). The coding process enabled the researcher to develop a plot that explains the study in relation to the primary category.

The three stages of coding identified above resulted in a thematic analysis of the qualitative data.

3.9.11 Constant comparison

---

There is a requirement for qualitative analysis to examine data carefully and explore all its dimensions. In analysing the data, the researcher therefore applied the grounded theory principle of constant comparison which requires a researcher to code each passage of text that is read and then subsequently compare it with all the passages that have previously been coded. The researcher found this approach beneficial because it enabled her to adopt a consistent approach to coding the data while giving her the opportunity to highlight aspects of the data that required alternative coding.

3.9.12 Inductive approach to coding

As the interviews produced a substantive amount of data and various common themes, the researcher coded some data in a bid to evaluate segments relating to emergent themes, ideas and perspectives. In coding the data, the researcher adopted an inductive approach to analysing the data. Inductive analysis entails a researcher being engrossed in details of the data to identify significant categories and aspects of a data as opposed to testing hypothesis derived theoretically.

The researcher applied the qualitative approach of content analysis. In doing so, she implemented a four-step process which involved pinpointing the themes, allocating codes to the primary themes, categorizing responses under the primary themes and assimilating themes and responses into the text of her report. Although the researcher found the task of analysing the data laborious due to the vast content of

498 Anslem Strauss and Juliet Corbin, ‘Grounded Theory in Practice’ (2nd edn Sage, 1998) 75
the data generated from the interviews, she ensured that she repeatedly read through the transcripts, recorded themes and searched through data for recurring conversations and possible patterns. The researcher adopted measures such as the use of coloured coded schemes, the use of highlighters, interview notes and excel spreadsheets. These measures enabled the researcher to discover an analytical direction which influenced her integration of the major themes in the data into her findings.

The researcher initially, coded the data manually. To this effect, it has been highlighted that manual coding enables a researcher to obtain a better literal perspective which may not be possible via electronic coding. Saldana suggests that a researcher might have more control of a given piece of research work if the qualitative data is on paper and coding is conducted manually via the use of pencil so to speak. Significantly, manual coding gives a researcher the option to hand code qualitative data by using a scheme based on colour coding and the cutting and pasting of text segments onto note cards.

On completing the manual coding, the researcher embarked on electronic coding by using the “find and replace” tool on the word Microsoft office tool to confirm the themes and organise the information generated by the manual coding process.

3.9.13 Ethical considerations

There is a requirement for ethical issues in qualitative research to be addressed with a view to protecting the interest of those participating in the study as a result of the research.\textsuperscript{503} Halai acknowledges that some of the research ethical issues include informed voluntary consent, confidentiality of information shared and anonymity of research participants. Against this backdrop, Corti and Blackhouse suggest that research should be conducted subject to the participants freely informed consent.\textsuperscript{504} In conducting the study the researcher ensured that her study was guided by ethical considerations. In doing so, the researcher protected the interest of the participants by implementing four measures. The first step that the researcher took was to obtain the approval of the senior management officials of the CPS and the MPS stakeholders who provided access to the prosecutors and police officers. Hence, it has been emphasised that gaining the consensus of individuals in authority to provide access to research participants is a vital ethical consideration for data collection.\textsuperscript{505}

The second measure that the researcher implemented to protect the interest of the participants was that on visiting the various research sites, she applied the principle of informed consent which has been highlighted as a significant ethical consideration which should guide a study.\textsuperscript{506} In doing so, the researcher notified participants of the nature of the study and informed them of their rights to participate in the study on a voluntary basis and to refuse to participate.

\begin{footnotes}
\item[505] John Creswell, ‘Research Design’ (3\textsuperscript{rd} edn Sage, 2009) 90
\item[506] Louise Corti , Annette Day and Gill Blackhouse, ‘Confidentiality and Informed Consent: Issues for Consideration in the Preservation of and provision of Access to Qualitative Data (2000) 1 Qualitative Social Research 3
\end{footnotes}
The third measure that the researcher implemented was to conduct the interview anonymously as requested by the participants. In doing so, the researcher respected the decisions of the participants not to have tape recorded interviews and recognised the concerns that the participants had raised due to the sensitive nature of their jobs. The researcher therefore protected the identities of the police officers and Prosecutors by using codes when analysing the data. Against this background, it has been highlighted that to protect the identity of participants, researchers may be required to conceal the identity of participants and places in the dissemination of the study.507

The fourth measure that the researcher applied was to uphold the principle of confidentiality by not divulging any information which was obtained during the interviews without the permission of the participants. In effect, the researcher ensured that she did not reveal any data gathered from the interviews with the law enforcement officials either deliberately or accidentally by being cautious at all times to safeguard the data.

In addition to the above, the researcher sought and received ethical approval from the University Academic School’s Research Committee for the School of Law. Based on the ethical principles, the researcher informed the participants prior to interviewing them of the nature of the research, the right to withdraw from the study and the fact that the study will be conducted on a voluntary, anonymous and confidential basis.

Chapter 4: Data analysis, findings and result

4.1 Introduction

This chapter explores the research findings from the interviews with the 63 law enforcement officials who took part in the study. The purpose of this study is to analyse the perceptions of police officers and prosecutors in London in relation to cyberstalking and what they consider to be the threshold of acceptable behaviour on the internet. A further objective of the research is to identify the perceptions of police officers and prosecutors in London in respect of the factors which frustrate them in the investigation and prosecution of cyberstalkers. In so doing, the study will seek to explore the following:

(a) The extent to which lack of knowledge and training hinder the investigation and successful prosecution of cyberstalkers.

(b) How the issues of anonymity and lack of resources can affect the risk assessment of both victims and cyberstalkers.

(c) The effects of evidential difficulties and victim behaviour on the investigation and successful prosecution of cyberstalkers.

The researcher interviewed various London law enforcement officials to obtain a cross-section of opinions. The research sample comprised of the following participants:

Owing to the need to ensure total anonymity the participants were allocated pseudonyms as below….

(a) 25 Police Officers PO (Numbers 1-25)

(b) 30 Crown Prosecutors PRO (Numbers 1-30)
4.2 The data

The study produced a large quantity of data due to the number of interviews that were conducted. The quantity of the data is justifiable because the data provided findings which are relevant to the research objectives. Further, the data reinforced commonly held views based on which the emergent themes were identified.

The interviews were transcribed using Saldana’s coding method which required the researcher to identify themes by looking for word repetitions, looking for key-words-in-texts, reading unmarked texts, and cutting up and sorting the transcripts.\textsuperscript{508} Saldana highlights that coding is a cyclical process.\textsuperscript{509} Specifically, the researcher applied Saldana’s cyclical approach to coding the research data based on five cycles of coding.

In addition to interviewing 25 police officers and 30 Prosecutors, the researcher interviewed 4 other UK law enforcement officials. These interviews produced additional data which were relevant to the study. The additional interviews enabled the participants to answer the researcher’s questions from the perspectives of a Member

\textsuperscript{509} Johnny Saldana, The Coding Manual For Qualitative Research (3rd edn ,Sage 20012) 45
of Parliament, parliamentary research assistant, probation officer and government policy adviser.

This data analysis chapter examines the backgrounds and experiences of the participants. The chapter also, explores the perceptions of the participants on what constitutes the threshold for distinguishing rudeness, abuse and unpleasant comments from cyberstalking on the internet. Additionally, this chapter discusses the perceptions of police officers and prosecutors in London on the perceived challenges that hinder police officers and prosecutors from risk assessing victims of cyberstalking. Finally, Chapter 4 discusses the perceptions of police officers and prosecutors on how lack of legislative difficulties, lack of knowledge, training and resources, risk assessment difficulties, evidential difficulties and victim behaviour frustrate police officers and prosecutors in the investigation and prosecution of cyberstalkers.

4.2. 1. The background and experience of the London police officers

Twenty-five police officers were interviewed for the research study. The police officers consisted of an assistant chief constable, 3 detective sergeants, a chief inspector, 15 detective constables and 5 police constables. The participants acquired the relevant experience while working in different departments of the MPS. The participants worked in various offices such as the department of the assistant chief constable, community safety unit, domestic violence unit, Police Central e-Crime unit, the extradition unit of New Scotland Yard and the Serious Organised Crime Agency. The research participants had a range of experiences pertaining to domestic violence cyberstalking, celebrity cyberstalking, online grooming, cyberstalking of a religious leader,
cyberstalking of a high ranking official and cyberstalking of strangers. The police officers provided useful data from a law enforcement perspective.

The researcher travelled to various offices in the UK to conduct the interviews. The offices included the police headquarters in Manchester, the Senior Organised Crime Unit and the Police Central Cyber e-Crime Unit. Additionally, the researcher travelled to New Scotland Yard, Acton and Kilburn police stations in London to conduct the interviews. The researcher conducted the interviews over a twelve month period.

The researcher asked the participants if they had any experience of investigating and prosecuting cyberstalkers. Tables 4.1, 4.2 and 4.3 respectively, depict the ranges of responses of the police officers. Of the 25 police officers, 15 had the experience of investigating cyberstalking cases involving strangers, 1 police officer had the experience of investigating a case involving online grooming and 7 of the police officers had the experience of investigating cases involving domestic violence. Additionally, 1 police officer had the experience of investigating cases involving a celebrity and another police officer had no experience of investigating a cyberstalking case. The respondent who had no experience of investigating a cyberstalking case however, confirmed that he had investigated fraud cases which had been committed digitally.

Table 4.1 below illustrates the various experiences of the police officers. Table 1 indicates that a majority of the police officers which is 60% out of 100% of the police officers had the experience of investigating cases involving strangers as opposed to 28% out of 100% of the police sample which had the experience of investigating
cyberstalking cases that were linked to domestic violence. The findings further suggest that some cyberstalking cases involve domestic violence victims.

**Table 4.1: Police officers experience of Cyberstalking by type**

<table>
<thead>
<tr>
<th>Experience type</th>
<th>Frequency</th>
<th>Percentage of Sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyberstalking</td>
<td>15</td>
<td>60</td>
</tr>
<tr>
<td>Online grooming</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Domestic violence</td>
<td>7</td>
<td>28</td>
</tr>
<tr>
<td>Celebrity</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>No Experience</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>25</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

The data in Table 4.1 further illustrate that 1 out of 25 police officers had the experience of investigating cases relating to online grooming. This demonstrates that online grooming can involve elements of cyberstalking. This is not surprising given that cyberstalking and online grooming both involve the harassment of victims via information and communication technology. The data in Table 4.1 additionally indicates that 1 out of 25 police officers had no experience of investigating cases on cyberstalking.

Out of the 25 police officers, 1 revealed that he did not prosecute cyberstalkers who disseminated offensive messages to colleagues and former partners because, he gave the culprits harassment warnings instead. The police officer stated that such perpetrators were let off on those occasions on the condition that they do not harass the victims again. The police officer also indicated that such perpetrators were warned
that they would be formally prosecuted if they re-offend. Importantly, the police officer stated that he gave cyberstalkers harassment warnings to give them another chance. Out of the 25 police officers, 2 others also discussed penalising cyberstalkers by giving them harassment warning notices. This demonstrates that depending on the facts of certain cases, police officers may decide to divert cases from the court system by sanctioning cyberstalkers through harassment warnings.\(^5\)

4.2.2: The background and experience of the London prosecutors

In addition to police officers, the researcher interviewed 30 prosecutors. The prosecutors comprised of participants who work in various departments of the Crown Prosecution Service (CPS) which include the Magistrates’ Court, the Crown Court department, the serious casework department and the rape and serious sexual offences department. The prosecutors consisted of Magistrates’ Court prosecutors, Crown Court prosecutors, rape specialists, higher court advocates and borough crown prosecutors. The borough crown prosecutors were in senior managerial positions. The prosecutors provided useful data from a managerial perspective given their legal backgrounds and experiences.

The researcher recruited diverse participants because there were no designated specialist cyberstalking prosecutors at the time of the study. The prosecutors had therefore acquired varied experiences of prosecuting cases involving aspects of cyberstalking in the general course of their jobs while working at various CPS offices.

\(^5\) Harassment warnings are usually given by police officers to suspects when a single act is alleged to have occurred in a bid to notify a suspect that his act has caused harassment and to warn the individuals that if a subsequent act is reported, the individual may be arrested and charged for the offence of harassment. Harassment warnings are not convictions or cautions.
The researcher interviewed the prosecutors during the second and third years of the study.

The researcher conducted the interviews while based at Isleworth Crown Court as a para legal officer. Due to the fact that there was no specialist cyberstalking department at the time of the study, the researcher interviewed a varied sample of prosecutors in a bid to obtain a cross section of views. As a result, the researcher travelled to the different CPS offices in Southwark, Croydon, London Bridge and Pimlico to interview the Prosecutors. Additionally, the researcher visited Isleworth, Snaresbrook and Inner London Crown Courts respectively to interview three higher court advocates. The higher court advocates are prosecutors who have been granted extended advocacy rights to present cases in the crown courts.

Due to the fact that there is no specific legislation in the UK on cyberstalking, most of the participants had reviewed the related cases of harassment, which encapsulates aspects of cyberstalking. The varied experiences of the prosecutors just like the experiences of the police officers were significant because different categories of cyberstalking victims were identified from the resulting data.

The data in Table 4.2 indicate that a majority of the participants (77% out of 100%) prosecutors had the experience of investigating cases involving the cyberstalking of strangers. The data in Table 4.2 further illustrate that a minority of the prosecutors, (1 out of 30 prosecutors to be precise), had the experience of investigating a fraud case involving an aspect of cyberstalking. In addition, the data in Table 4.2 indicate that 4
out of 30 prosecutors had experience of prosecuting cyberstalking cases involving domestic violence.

The data in Table 4.2 further reveal that a majority of the prosecutors had the experience of investigating cyberstalking cases as opposed to a minority of the sample which had the experience of investigating cases involving celebrities. This suggests that like the police officers, the sample of prosecutors had a wide range of experiences. The findings further reveal that there are similarities in the experiences of the police offices and the prosecutors. In particular, the participants in both samples had more experience of investigating cyberstalking cases involving strangers in comparison to cases involving former partners. A high percentage of the sample had investigated cyberstalking cases involving strangers and domestic violence.

The data in Table 4.2 show that in congruence with the experience of the Police officers the majority, (77% out of 100%), of the sample of prosecutors had the experience of investigating cases on cyberstalking involving strangers in comparison to just 7% out of 100% of the sample of prosecutors which had the experience of investigating cases involving celebrities.
Table 4.2: Prosecutor's experience of Cyberstalking by type

<table>
<thead>
<tr>
<th>Experience type</th>
<th>Frequency</th>
<th>Percentage of sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyberstalking of strangers</td>
<td>23</td>
<td>77</td>
</tr>
<tr>
<td>Domestic Violence</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>Celebrity</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Fraud</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>30</td>
<td>100</td>
</tr>
</tbody>
</table>

4.2.3 The background and experience type of the UK law enforcement officials

To obtain the perspective of a government official on the research topic, the researcher visited Portcullis House in Westminster to interview a Member of Parliament and a parliamentary research assistant. The participants provided insights on the research topic from the perspective of government officials tasked with reviewing the effectiveness of the stalking legislation in the UK.

To obtain the views of other criminal justice officials, the researcher interviewed a senior UK chief executive of the national probation office who had assisted the government in implementing legislation on stalking in the UK. The interviewee provided an insight on the research topic from the perspective of the probation service.

In addition to the above, the researcher travelled to Northern Ireland to interview a government policy adviser with a view to obtaining their perspective on the best
working practices. The interviewee was responsible for advising the Northern Ireland government on the enactment of legislation to regulate new criminal behaviours. The interviewee provided useful comparative data given that stalking is not yet a specific, criminal offence in Northern Ireland. The participant informed the researcher that in Northern Ireland due to political tensions in the country at the time of the study, the focus on cybercrime for government officials was in relation to terrorism.

The data in Table 4.3 indicate that 3 out of 4 UK law enforcement officials had experience of dealing with cases involving harassment. The data in Table 4.3 further indicate that 1 UK law enforcement official had the experience of dealing with cases involving cyberstalking. It should be noted that at the time of the study, the term harassment connoted either face to face stalking or cyberstalking and was at times, used interchangeably.

Table 4.3: Government Official’s Experience of Cyberstalking by type

<table>
<thead>
<tr>
<th>UK Law Enforcement Officials</th>
<th>Experience Type</th>
<th>Frequency</th>
<th>Percentage of Sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member of Parliament</td>
<td>Harassment</td>
<td>1</td>
<td>25</td>
</tr>
<tr>
<td>Research Assistant</td>
<td>Harassment</td>
<td>1</td>
<td>25</td>
</tr>
<tr>
<td>Probation Official</td>
<td>Cyberstalking</td>
<td>1</td>
<td>25</td>
</tr>
<tr>
<td>Northern Ireland Official</td>
<td>Harassment</td>
<td>1</td>
<td>25</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>4</td>
<td>100</td>
</tr>
</tbody>
</table>
The data in Table 4.3 depict the various backgrounds of the 4 UK law enforcement officials. The data illustrate that 2 out of 4 law enforcement officials were affiliated with Parliament at the time of the study and that 1 of the law enforcement officials was a probation official who was an executive official of the UK national probation agency at the time of the study.

**4.2 Data from interview transcripts of the prosecutors and police officers—significant themes**

The data from the interview transcripts were analysed using the coding methods previously described. The analysis produced several main themes. The views of the participants have been paraphrased in this chapter to support the themes. The themes identify some of the perceptions of London police officers and prosecutors on cyberstalking and the threshold of acceptable behaviour on the internet. Most of the participants highlighted several factors which distinguish rudeness, abuse and unpleasant comments from cyberstalking. The themes also reveal the issues that frustrate London police officers and prosecutors in the investigation and successful prosecution of cyberstalkers.

The seven main themes that emerged are ‘threshold of acceptable online behaviour’, ‘legislation’, ‘lack of training and knowledge’, ‘lack of resources’, ‘risk assessment challenges’, ‘evidential challenges’ and ‘victim behaviour’. The findings are discussed in relation to the main themes. The themes presented in this chapter are validated by
extracts from the data. The participants who took part in the study were given participant codes in order to provide anonymity and retain confidentiality.

4.2.1 Theme 1: Threshold of acceptable online behaviour

As previously shown, the participants had various experiences of investigating and prosecuting cyberstalkers in both domestic violence and non-domestic violence cases. Given the varied experiences of the participants with different types of cyberstalking, the majority of the participants discussed the thresholds for distinguishing routine rudeness, abuse and unpleasant comments on the internet from cyberstalking. The majority of the participants stressed that they perceived there to be various thresholds for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking.

The findings of this study reveal that all the police officers and 96% of the prosecutors shared the perception that various factors ought to be considered when determining the threshold for distinguishing between rude, abusive and unpleasant comments on the internet and cyberstalking. Further, the findings as contained in Tables 4.4 and 4.5, reveal that the police officers and prosecutors identified between 9 and 11 different factors which they perceive distinguish rudeness, abuse and unpleasant comments on the internet from cyberstalking.
Table 4.4: Perceptions of prosecutors on the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from Cyberstalking:

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Number of prosecutors</th>
<th>Percentage of sample of prosecutors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subjective view of the victim</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>Objective Test</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Content of messages</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Intention of cyberstalker</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Impact on victims</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>Reaction of victims</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Statutory definition</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Duration of the conduct</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>Cyberstalker’s awareness of the impact on victims</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Gravity of the offence</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Vulnerability of victim</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>29</td>
<td>96</td>
</tr>
</tbody>
</table>
Table 4.5: Perceptions of police officers on the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from Cyberstalking:

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Number of police officers</th>
<th>Percentage of Sample of police officers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subjective view of the victim</td>
<td>7</td>
<td>28</td>
</tr>
<tr>
<td>Objective Test</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Facts of a case and motives of the Cyberstalker</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Impact on the victim</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Statutory definition</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Intention of the Cyberstalker</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Duration of the conduct</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>Size of the electronic platform that was used to disseminate messages</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Prior relationship with the victim</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Total</td>
<td>25</td>
<td>100</td>
</tr>
</tbody>
</table>

The participants acknowledged that the threshold depends on the Subjective Test as defined in Chapter 2 (section 2.2). Hence PO20 said “it depends on how the message was perceived by the recipient”. PRO22 echoed the view of PO20 that the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking is the Subjective Test. Therefore, in his extract, PRO22 emphasised that not all individuals might be bothered by the same offensive messages of a cyberstalker;
PRO22: “The test is subjective. For example, if you put 12 people in a room and put up offensive comments about them from a cyberstalker, 6 might be bothered and 6 might not be bothered by the same offensive messages”.

PRO17 shared the perception of PO20 and PRO22 that the threshold will depend on the Subjective Test. Therefore, PO17 stated that the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking is “the victim’s perception”.

**Int:** What in your opinion is the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking?

**PRO17:** “It boils down to the victim’s perception. Does the victim feel the conduct is causing her alarm? You have to take the victim’s account or reaction into play. It is a Subjective Test. would the victim find the conduct offensive?”

Similarly, the participants perceived the reaction of victims to be the threshold. Hence, PO18 echoed the views of PRO17, PO20 and PRO22. Hence PRO18 said in the last statement of his extract, “I think it depends on the victim”.

**PO18:** “I think it depends on the victim. I investigated a case which involved a cyberstalker who set up as negative fan mail page about the victim. The victim in this case was not particularly bothered by the negative comments and only wanted the cyberstalker to be stopped. I had another case which started off as an anonymous case and then developed into a personal attack. The cyberstalker in this case hacked into the victim’s computer and posted false malicious messages about the victim online and on Facebook. The victim in this case was severely affected by the actions of the cyberstalker unlike the previous case that I dealt with. So as you see, it depends on the individual”.

Similarly, the participants shared the perception that the threshold will depend on the impact of the behaviour on the health of victims. Hence, PROB1 expressed the view that the question to be asked in determining the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking is whether the victim was psychologically damaged. PROB1 indicated in his extract that it will also
have to be ascertained “if the harassment has caused the victim to change her normal routine”;

PROB1: “It depends on the impact on the victim. Is the victim damaged psychologically? If the harassment has caused the victim to change her normal routine then this is significant. For example, there was a cyberstalking case that resulted in the victim suffering from anorexia. The effect of the conduct indicates a progression from rudeness and unpleasant comments to outright cyberstalking”.

While discussing the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking, a minority of the participants made a distinction between cyberstalking victimisation in relation to celebrities and cyberstalking victimisation in relation to the general the public. In doing so, the participants attributed the threshold to “where an individual sits with society” (PO2) and “people in the limelight” (PO12).

Remarkably, PO2 asserted that celebrities have an ulterior motive for reporting cyberstalking victimisation which might lead to a false public expectation. PO2’s extract below echoes the view of the participants;

PO2: “It depends on the impact on the victim. An individual may regard an online abuse or harassment as ‘water off a duck’s back’ whereas another individual may be distressed by the same online abuse or harassment and will contact the police as a result. It also depends on where an individual sits with society”.

Int: Follow-up Question: What do you mean by it also depends on where an individual sits with society?

PO2: “Victims that have high positions or that are celebrities report such incidents because they expect that it will be investigated because of their standing in society. They also do so because they want to be seen taking a stand against the conduct. This gives a false expectation to victims who are part of the general public because they will not receive the same treatment when they approach the police for help after being subjected to the same online abuse that has been experienced by the celebrity”. It was not evident from the
interview why the police made this point. Suffice it say that the assumption that could be made is that a victim’s social or societal standing may affect how a cyberstalking incident is investigated.

While discussing the threshold, some of the participants shared the perception that “it is a matter of intent and depends on the motives of the cyberstalker” (PO23). However in contrast, PO12 in his extract, expressed the view that because cyberstalking is not done face to face, “a cyberstalker may be unaware of the impact that his conduct has on a victim”;

PO12: “There is the possibility that the cyberstalker committed the malicious acts without the intention of harassing the victims or without the knowledge that the victims have perceived the conduct as harassment. So, under the definition of cyberstalking, how can someone be accused of committing a malicious act when he is not aware of how the act is perceived by the recipient? In my view a cyberstalker may be unaware of the impact that his conduct has on a victim because unlike face to face stalking, it is hard to judge the immediate reaction of the victim or to access the impact that a conduct might have on a victim in the virtual world”.

PRO15 questioned how a person can be accused of committing a malicious act when “he lacks the requisite intent and is therefore, unaware of the impact that his conduct has on a victim”. The researcher however argues that a cyberstalker’s lack of awareness of the impact of his conduct on victims, should not constitute a defence for his criminal actions;

Like PO12’s, PO19 said that a cyberstalker “may be unaware of the effect of his actions on victims because there is no face to face interaction”. Also, PO25 said that “cyberstalkers may lack knowledge that their acts are perceived as harassment by victims”.

196
Furthermore, PO8’s extract echoed the perceptions of the participants that there is a possibility that cyberstalkers commit malicious acts without the intention of harassing victims.

PO8: “In the cases involving cyberstalking, the perpetrator may not have the intention to cause alarm or distress. Whereas in cases involving rudeness, abuse or unpleasant comments on the internet, the perpetrators may have the specific intention of offending the perpetrator. Cyberstalking is unlike face to face stalking where the stalker can immediately tell from the body language of the victim that the victim has been offended. In cyberstalking cases, it is not easy for one to make that distinction because the cyberstalker is hiding his or her identity behind a computer gadget and cannot physically see how the victim is being affected by their actions”.

The above extract suggests that the participants considered the issue of cyberstalking victimisation from the perspective of the cyberstalkers who were perceived as unable to assess the impact of their conduct on victims.

The participants also revealed that the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking, will depend on the effects of cyberstalking on victims. Hence, PRO24 in his extract, said that the threshold depends on “if the comments cause alarm or distress”;

PRO24: “Any abuse, rudeness and unpleasant comments on the internet will be equivalent to cyberstalking if the comments cause alarm or distress”.

PRO21’s extract which echoed the views of the other participants, and further serves to illustrate this point;

PRO21: “I think that there is a fine line between something deemed rude and a message that is perceived to be cyberstalking. In my view, if one is alarmed by
it and it causes alarm or distress, it is an abusive conduct. The threshold depends on the perception of the person on the receiving end”.

While discussing the threshold, an important theme that emerged from the accounts of the participants is that an individual may be upset by a cyberstalking incident and another person may choose to ignore it. Hence, PO10 said “a person might find a conduct offensive and another person will not”. Likewise, PRO20 remarked “an act that is construed as harassment by one victim may be considered as nuisance by another victim and trivialized”. Similarly, PRO27 expressed the view that the threshold depends on “how people choose to react”. Notably, PRO27 suggested that;

PRO27: “The threshold for distinguishing between rudeness and cyberstalking depends on individuals and how they choose to react. Some people choose to do nothing and wait. The level of harassment is crucial. Sometimes, the best way is not to react as cyberstalkers want to provoke a reaction. It all depends on the circumstances of the victim”.

In contrast to the above views, many of the participants believed that the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking is the ‘Objective Test’ or ‘Reasonable Person Test’. These tests ask if an ordinary person in the victim’s position would have reacted in the same manner as the victim. Consequently, PO6 in discussing the threshold, questioned whether “a reasonable person in the victim’s position will be offended”. Worryingly, PO6 expressed the view that victims have the option of switching their computers off to avoid being bothered by cyberstalkers;
PO6: “The Reasonable Person Test. The question to be asked is would a reasonable person in the victim’s position be offended? If for example I am sent an abusive message online my personal individual reaction will be to turn off my computer or stop using the computer entirely if needed. Other people who receive the same abusive message may perhaps, be sensitive and seek help of the police to get to the bottom of it”.

Like PO6, PO23 stated that the threshold has to “pass the Reasonable Person Test”. The Objective Test is the same as the Reasonable Person Test. PRO19 agreed with PO6 and PO23 that the threshold will depend on the Objective Test. However, PRO19 highlighted that “there should be a respect of the right to freedom of expression as long as the criminal threshold is not passed”.

PRO19: “I think you have to have an objective approach to it. There has to be an impartial analysis of the situation as some people may take it personally and others are not bothered. Because the internet is full of people with opinions, it sets the threshold of when we prosecute very high. There should be respect of the right to freedom of expression as long as the criminal threshold is not passed”.

The criminal threshold for stalking is highlighted under S2A of the PHA (1997) and S4A of the PHA (1997). Section 2A of the PHA defines the offence of stalking as pursuing a course of conduct which amounts to harassment and stalking.\textsuperscript{511} Section 4A of the PHA (1997) creates the offence of stalking involving fear of violence or serious alarm or distress. The offences were previously discussed in Chapter 2, sections 2.3.3 and 2.3.4 respectively. The criminal threshold is defined by the relevant legislation and will therefore be met once either of the above highlighted offences are committed.

\textsuperscript{511} A course of conduct is the same as defined under section 7 of the PHA 1997 and referred to elsewhere in this guidance
Like PO6, P019 and PRO23, PRO25 shared the perception that the Reasonable Person Test will be used to distinguish between rudeness, abuse and unpleasant comments on the internet and cyberstalking. However, PRO25 added that he would also, take on board the views of victims.

PRO25: “I would consider the views of the victim together with some form of Objective Test. We need to take on board the views of the victims”.

From a legal perspective, whilst discussing the threshold in relation to the culpability of mentally ill cyber stalkers, PRO28 cited the case of R v Colohan.\(^{512}\) The principle established in the case of R v Colohan suggests that it may be difficult for cyber stalker to evade liability on the grounds of a mental health condition.

PRO28: “In the case of Colohan, the defendant appealed against his conviction for harassment on the grounds that he was suffering from Schizophrenia. However, the court held that the mental health condition of the defendant was irrelevant and not a defence because an objective test had to be applied when determining whether the actions of a mentally ill individual constitutes harassment because the question that ought to be asked is whether a reasonable person would think that the actions of the individual amounted to harassment.”

In contrast to the participants who shared the perception that the threshold will depend on either the subjective or the reasonable persons test, PRO29 said “I am not sure if the Objective Test or the Subjective Test should be applied”.

*Please note the Reasonable Person Test is discussed in Chapter 2, section 2.3.5.*

---

\(^{512}\) [2001] All.ER 230
Notably, while discussing the threshold and the culpability of cyberstalkers from a legal perspective, PRO29 said that cyberstalkers were legally required to take their victims as they found them. This perception implies that that cyberstalkers will be held responsible for the impact of their behaviour on victims regardless of whether any adverse effects were foreseen:

PRO29: “In the case of R v Blaue, the principle of take your victim as you find him was established. It does not matter that another person would have shaken the cyberstalking behaviour off. You see I am not sure if the Objective Test or the Subjective Test should be applied. I say take your victim as you find him”.

Like PRO29, PO15 discussed the vulnerability of victims. Hence, PO15 remarked “you will have to ask whether the cyberstalker sought a vulnerable victim”.

PO15: “The perception of the person on the receiving end is crucial. Others will argue in assault allegation take your victim as you find him. You will have to check whether the defendant sought out a vulnerable victim”

From the outset of the study, it was evident that given their prosecutorial backgrounds, the prosecutors who took part in the study would identify the statutory provisions as the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking. Consequently, PR014 said that the threshold will depend on “whether the behaviour is legally defined”. When asked why he held this view PR014 explained that when a conduct is defined in law, it is perceived to be serious. In expressing this view in his extract, PRO14 made a distinction between a racial incident which is based on “what the victim perceived” and cyberstalking which is “based on the legal definition of the behaviour”;
PRO14: “It has to be legally defined. It is not all about the subjective perspective. It has to be what about the law says that can count regardless of whether I think that it is rude or cyberstalking. When defined in law, the conduct prohibited in law will be viewed as serious. In some of the cases like racial harassment the conduct is defined on a subjective basis. A racial incident is subjective. An incident can be racial to me but not to you. It is based on what the victim thinks or perceives at that point in time but for harassment and cyberstalking cases the threshold should be defined by law.”

In agreement with PRO14, PRO27 shared the perception that the threshold will depend on the wording of the statute. PRO4 however, identified when a cyberstalking case has an aggravating factor;

PRO27: It is a matter of referring back to the wording of the statute. If the conduct is done on more than one occasion, it will amount to stalking and cyberstalking as the case may be. When the cyberstalker has been put on notice that his unwanted conduct is upsetting the victim and he still carries on, then the aggravating factor occurs where the cyberstalker ignores the personal feelings of the victim and still carries on with the conduct.

Similarly, PRO16 shared the perception that the threshold “will depend on the definition of the terms of the Act;

PRO16: “Multiple comment crosses the line of being harassment. It will depend on the definition of the terms of the Act. It will be the cause of conduct. The test is that it must have occurred on more than one occasion”.

Likewise, PRO11 shared the perception that the threshold will depend on statutory provisions. Hence PRO11’s extract echoes the views of the other participants;

PO11: “The intensity and duration of the activities is the dividing line. This is provided for in the legislation as stalking has to be a course of conduct which means that by law, it has to be done on more than one occasion. If it is a one off act, the Malicious Communications Act will be applicable but if it is an intense long term act, then the Protection from Harassment Act will apply”.
Similarly, PRO21 shared the perceptions that the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking is the “the legislation” in addition to the “reaction of victims”;

PRO21: “I think it all depends the perception of each individual. The focus should be each individuals’ reaction. The criteria for cyberstalking will be met when aspects of the legislation has been satisfied”.

While discussing the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking, many of the participants stressed that it will be determined by the frequency of events as opposed to the nature of the comments. Hence PRO3 remarked “we need to look at the frequency rather than the nature of comments”. PRO3’s extract echoes the views of many of the participants.

PRO3: “Stalking is a pattern of events and so we need to look at the frequency rather than the nature of comments to distinguish it from rudeness, abuse and unpleasant comments”.

PRO7 shared the perception of PRO14 and PRO3 that the threshold depends on the duration of the behaviour; “the threshold depends on if there is a “repetition of the conduct” (PRO7). Similarly, PO13 stated that the threshold depends on whether the activity of a cyberstalker “goes over a couple of messages and is a continued action”. Likewise. PO16 said the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking depends on if the incident occurred on “more than one occasion”.

203
PO20 in his extract, echoed the views of PRO14, PRO3 and PRO7. Particularly, PO20 made a distinction between “persistent incidents” and a “one off comment”;

PO20: “I think for it to be cyberstalking, it has to involve persistent incidents as opposed to a one off comment. It has to be a repeated conduct over a period of time and not a one off rudeness”.

Like PO20, PO25 made a distinction between “repetitive behaviours” and “isolated incidents”;

PO25: “The offence will have to be one that was done on more than one occasion. Their cyberstalking behaviour has to be repetitive and not just an isolated incident. …It has to be done over a given period or length of time for it to amount to a cyberstalking incident”.

Akin to PO25, PRO13 in his extract, expressed the view that the threshold will depend on whether the “conduct is repeated”. However, PRO13 added that it depends on whether there exists “a clear indication that the conduct is unwanted”. Similarly, PRO12 expressed the view that the threshold depends on if the victim asked the cyberstalker to stop. However, PRO12 also added that additional factors to be considered are the content of the messages and the frequency of the conduct;

PRO12: “It is how the victim and the other people perceive it. If the defendant is rude, persistent and offensive then it becomes cyberstalking. It also depends on if the victim asked the cyberstalker to stop. It will still be considered cyberstalking even if the messages are not rude especially if it is done in public. I know that people say that if a rude message is posted online, the recipient should look not look at it but my argument is that you have to look at the content of the message to know the threat level in case it escalates to more serious
actions like threat to life. If you are a victim, it is not as simple as saying do not look at the messages. She might be able to gain a hint of future threats”.

In agreement with PO12, other participants believed that the contents of the messages sent by cyberstalkers was the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking. Hence, they said the threshold depends on “if the messages are sinister” (PO4) and “insulting” (PO7).

While discussing the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking, PRO29 expressed the view that if there is “escalation in the abuse” such behaviours will constitute cyberstalking. Likewise, PRO22 stated that the threshold will depend on if the cyberstalking behaviour “crossed the line”. Notably, PRO22 in his extract, equated crossing the line to when comments “become menacing”;

PRO22: “The law says that the line is crossed when it becomes menacing. In such instances, we need to balance the right to freedom of speech against causing alarm, distress or harassment. That is where the line is drawn. In one case that I reviewed, a female harassed the ex and sent emails, letters and stuff on Facebook. When the ignored her, she took it to another level calling him a paedophile and then sent text messages begging him to take her back. It was not a criminal activity when she was sending messages begging to get back with him until she realized that he was not interested. She enlisted the help of her friend to print out the letter and hand it out to everyone in the community that he was a paedophile. She was convicted and her friend was charged with joint enterprises and harassment by defamatory letters in the letter boxes of neighbours”.

Like PRO22, PRO26 expressed a shared perception that the threshold will be dependent upon whether the conduct of a cyberstalker is “grossly offensive”. 
However, both PRO22 and PRO26 raised the issue of the right to freedom of speech and expression when discussing the threshold;

PRO26: “The test is that it has to be grossly offensive. We had a case where the defendant was alleged to have posted comments on Facebook saying that the victim was a slag. There was a huge debate surrounding this case because people said no as you have to protect the freedom of speech and expression. The standard is high for that reason”.

Similarly, PO23 explained that “the problem is that there is a fine line between freedom of speech and the right to online privacy in an online medium that is designed to have worldwide publication”.

Some of the participants shared the perception that the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking were linked to the “the facts of the case” (PO15) and the “size of the electronic platform that was used to disseminate messages” (PO20). Similarly, PO17 asserts that the type of the electronic platform and the size of the audience were relevant. PO17 however, made a distinction between messages that have been posted on a private forum and messages that have been posted on a public forum;

PO17: “If the malicious message was posted on a private forum there is no problem as such because only a limited number of people will view it but if the message is posted on a public forum then there would be a problem because there will be a much wider audience”.

The researcher does not agree with PO17’s stance because a victim may still be subjected to abuse at the hands or a cyberstalker even if offensive messages are posted on a private forum. Supporting this point, PO2 while discussing the threshold,
highlighted that the problem with online harassment is that “there is a level of permanence attached to the messages”.

While discussing the threshold, there was consensus among the participants that cyberstalking is not taken seriously because it is carried out online. From a governmental perspective, MEP therefore said “there needs to be a change in the cultural attitudes of people to the offence. People do not recognize the seriousness of the offence”.

Similarly, PO8 stressed that “law enforcement agencies should begin to take the offence seriously given the devastating effects it has on victim”. In the following interview sequence PO13 echoed the views of MEP and PO8 in explaining why cyberstalking is not perceived to be as serious as face to face stalking;

Int: What in your opinion, are the issues with cyberstalking that need to be addressed?

PO13: “I think it is not deemed to be as serious as face to face stalking or harassment”.

Int: In your opinion, why do you think that is the case?

PO13: “There is no contact with the victim. We tend to look at the potential damage to victims when investigating such cases”.

Int: Would it be right to infer that such a balancing exercise tends to reveal that such cyberstalking cases complained of are not deemed to be serious in your opinion?
PO13: “That’s right. It all depends on if there is a potential risk to the victim. If not…….With face to face stalking the risks are obvious but with cyberstalking, we have to identify the risk…….It is not that straightforward”.

Like PO13, PRO20 expressed the view that cyberstalking is not considered a serious offence. Notably, PR20’s extract echoes the frustration of the participants and additionally highlights why cyberstalking should be regarded as a serious offence:

Int: What in your opinion are the issues with cyberstalking that need to be addressed?

PRO20: “The way that it is regarded by people generally. Not serious enough. The perception needs to change in my view because the conduct can be distressing for victims”.

It is important to note that whilst discussing the threshold, a minority of the participants referred to cyberstalking incidents which are committed as part of other offences. Hence, PO7 referred to “homophobic and racist cyberstalking offences”;

PO7: “It all depends on what was said and the length of time that the conduct spanned over. Single comments can be ignored. Homophobic and racist puts it into a different bracket”.

Comparably, a minority of the participants shared the perception that a threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking cannot be identified because cyberstalking is not a serious offence in comparison to other offences. Therefore, from a moral perspective, PO17 suggested that cyberstalking cannot be compared to offences such as selling drugs to children. PO17 however, acknowledged that the related offence of “cyberbullying leads to
suicide among victims and is widespread among children because children have easy access to social media”;

Int: What criminal category will cyberstalking be prosecuted under?

PO17: “If you are talking of trolling, it is distasteful and causes lot of distress on the victim. Although the victim impact is severe you cannot compare it to someone selling drugs to kids. Morality issues and the impact of a conduct on the victims make the selling of drugs to kids more serious than cyberstalking or posting malicious messages online”.

The participants expressed frustration that cyberstalking is considered to be less serious in comparison to other offences despite the fact that it results in the death of victims. Hence, PRO10’s extract echoed the frustrations of the participants;

Int: What suggestions do you have to assist the cross jurisdictional investigation of cyberstalkers?

PRO10: “Most people think that theft, murder, and rape are inappropriate, serious, offences. However, cyberstalking does not evoke the same condemnation even tough offenders end up murdering victims in some cases. I suspect that over the years, the behaviour will receive universal condemnation”.

PRO18 reiterated the views of the participants that cyberstalking is not perceived as a serious offence in comparison to face to face stalking. PRO18 highlighted that the there is a misconception that cyberstalking has a lesser impact on victims in comparison to face to face stalking;
PRO18: “I do not think that cyberstalking is given the same attention as face to face stalking on a one to one level. One to one physical level, face to face stalking is perceived to have a greater impact on the victim whereas, cyberstalking on a one to one level is perceived to have a less significant impact on victims. This is a totally wrong perception to hold. These are the issues with the definition of cyberstalking that need to be addressed. That is why a lot of societies distance themselves from the act which I think is wrong. I find it infuriating that there is an ignorance among certain aspects of society on the devastating psychological, emotional and mental effects that cyberstalking can have on victims. There is a dangerous misconception that because cyberstalking is not physical, it is less serious”.

While discussing the difficulty of identifying a threshold, MEP cited the case of Paul Chambers to suggest that in the cyber world, it is difficult to tell if a person is joking.

Int: What in your opinion is the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking?

MEP 1: How do you determine the threshold? That is the problem. You recall the case of an airport passenger who threatened to blow up the airport if he was not let out of the airport. In that case it was difficult to tell if the passenger was joking or if he really meant to carry out his actions. The passenger Paul Chambers was convicted of sending a menacing tweet threatening to blow up Doncaster airport. He sent the Tweet as a joke on Twitter. On 27/7/12, he won a High Court appeal victory after his conviction was quashed by three High Court judges. This case indicates the difficult balancing test that needs to be applied by the courts which weighed up, threats to the safety of the airport passengers against the requirement for all staff to notify the police of any serious security threats that have been made by members of the public to the airport passengers and staff.

The majority of participants shared the perception that there should be a threshold for acceptable online behaviour. Further, they expressed concern that vulnerable victims such as young girls, accept things online which they do not accept in person. Hence, PO1 remarked that “the threshold of acceptable online behaviour is shocking and should be looked at to tackle offending”.

210
In conclusion, the participants shared the perception that the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking depends on different factors. Most of the participants, recognised that individuals may respond differently to cyberstalking victimisation. Some of the participants therefore, used the following analogies to describe the reaction of some unperturbed victims to cyberstalking victimisation “water off a duck’s back” (PO2), “thick skinned” (PO3) and “not bothered” (PO20). These terms indicate that the participants shared the view that people react differently to cyberstalking victimisation and arguably suggests that some victims may not affected by victimisation while others may not be. There was no indication from the study that police officers and prosecutors were not taking the issue of cyberstalking seriously despite the fact victims react differently. On the contrary, there was an indication that the police officers felt that some victims perceive cyberstalking to be a minor offence and therefore, are reluctant to report incidents to the police because they believe that police officers which will not take cyberstalking incidents that are reported seriously.

4.3.2 Theme 2: Legislation

‘Legislation’ was the second theme identified through analysis of the data. Given the various background experiences of the participants, the perceptions of the participants on the criminalisation of cyberstalking as an aspect of cybercrime were varied. The findings of this study reveal that 92% of the police officers and 90% of the prosecutors shared the perception that certain legislative issues frustrate them in the investigation and prosecution of cyberstalkers. The legislative issues include perceived leniency in sentencing, the implementation of existing legislation, underreporting, breaching of
restraining orders, establishing a course of conduct under the PHA, establishing fear of violence under the PHA, and the statutory time limit for commencing proceedings under the Protection from Harassment Act (1997).

Furthermore, the findings as contained in Table 4.6 reveal that the police officers and prosecutors identified 6 and 9 perceived legislative issues respectively which frustrate them in the investigation and prosecution of cyberstalkers.

Table 4.6: Perceptions of police officers and prosecutors on Legislation:

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Number of police officers</th>
<th>Percentage sample of police officers</th>
<th>Number of prosecutors</th>
<th>Percentage sample of prosecutors</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHA lenient sentencing options</td>
<td>6</td>
<td>24</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>Ineffective legislative implementation</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>No single cyberstalking legislation</td>
<td>3</td>
<td>12</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Restraining orders are breached</td>
<td>2</td>
<td>8</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>Establishing course of conduct under the PHA</td>
<td>6</td>
<td>24</td>
<td>9</td>
<td>30</td>
</tr>
<tr>
<td>Statutory time limit for prosecuting</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Definition of cyberstalking</td>
<td>4</td>
<td>16</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>23</td>
<td>92</td>
<td>27</td>
<td>90</td>
</tr>
</tbody>
</table>
A majority of the participants shared the perception that several legislative issues hinder them in the investigation and prosecution of cyberstalkers. From the outset of the study, it was evident that the participants were frustrated by lenient sentences which they perceived were given to convicted cyberstalkers. Hence, PO16 when asked how effective the laws in the country are said “there should be stronger sentencing laws to protect victims”. Furthermore, PO16 expressed frustration at the perceived problem of lenient sentencing which “results in victims getting a raw deal”.

Int: How effective do you think that the laws in this country are against cyberstalking?

PO16: “When cyberstalkers are charged and successfully prosecuted, sometimes judges impose restraining orders to prevent the cyberstalkers from contacting victims further. Generally we will love to have all the laws to be tougher as we believe that the criminal justice system is soft on the accused who often receive lenient sentences. This results in victims getting raw deals”.

Like PO16, PO23 expressed the view that cyberstalkers should be given stronger sentences to protect victims. However, PO23 attributed the issue of lenient sentences to lack of judicial knowledge on the seriousness of cyberstalking and the impact that the behaviour has on victims;

PO23: “Harsher sentences should be passed when cyberstalkers are found guilty to pass on the message that the behaviour is abominable. The judges and jurors should be enlightened on the seriousness of the offence to enable them to pass adequate sentences. They should be trained on the devastating effects that it has on victims”.

The participants expressed frustration that the existing legislation is not adequately implemented. Particularly, they raised concerns that victims delay in reporting
incidents. Consequently, PO1 stated that the reluctance of victims to report incidents will make it difficult to assess the effectiveness of existing laws;

PO1: “I think we have one of the best pieces of legislation in the world. The difficulties lie in the implementation of the legislation. What we need to do, is improve the ability to investigate the crime. From the victim’s perspective, the victim will experience an average of 100 episodes of stalking activities including cyberstalking before reporting the offence. The reluctance of victims reporting the conduct makes it difficult to assess the effectiveness of the legislation”.

Like PO1, PRO4 expressed the view that the laws were adequate and that the problem was in implementing the existing laws. Notably, while discussing the issue of existing legislation, PRO4 highlighted that police officers also make decisions to charge offenders in harassment cases;

PRO4: “The legislation is effective. However, there are many cases that we won’t see as the police are making a lot of the decisions with our input. It is a two staged process. Sometimes, the police charge harassment cases where a conduct has only been committed once. There are some evidentially good harassment cases where the defendant hasn’t been charged. It is a matter of implementing it”.

In contrast to PRO4, PROB stressed that “the current law and practice are ineffective”;

PROBHF: “At the moment, it is completely ineffective. The current law and practice are ineffective”.

Likewise, PRO5, echoed the view of PROBHF and stated that “there were no effective laws”. Notably, PRO5 in his extract, linked effectiveness of laws to “adequate enforcement”.

Int: What difficulties do the police face in the investigation of cyberstalkers?
PRO5: “There are no effective laws. The effectiveness of law depends on adequate enforcement”.

While discussing the existing laws, PO18 said that the laws are only effective in cases “when it involves a racial element or aggravating factors”. It is important to note that only PO18 held this view.

Question: How effective do you think that the laws in this country are against cyberstalking?

PO18: “I do not think they are very effective or being enforced properly. It is only important when it involves a racial element or aggravating factors. When balanced against other problems that the police have ineffective legislation is a problem”.

The participants expressed frustration that there is no specific legislation for cyberstalking.

Int: What in your opinion are the issues with definition of cyberstalking that needs to be addressed?

PO9: “There is no specific legislation criminalizing cyberstalking. There is for stalking but not cyberstalking expressly. There needs to be a specific legislation defining the crime”.

Like PO9, PO12 stated that “there needs to be a specific legislation defining cyberstalking”. PO12 also indicated that a major issue is not being able to apply existing legislation to cases involving anonymous cyberstalkers. PO12’s extract echoes the views of the other participants;

PO12: “There needs to be specific legislation defining the crime. I think you have cyberstalking cases where the defendant is not known that is what comes to mind. The major problem for police officers is investigating anonymous
cyberstalkers and applying the law to such offenders whose identities are unknown”.

Like PO12, PO24 expressed the view that “there is insufficient legislation” to regulate cyberstalking. Similarly, PO24 acknowledged that despite the perceived issue of insufficient legislation, it is difficult to identify anonymous cyberstalkers. Particularly, PO24 explained that victims may be unaware that they are being targeted;

Int: What in your opinion are the issues with defining cyberstalking that need to be addressed?

PO24: “There are I would say, insufficient legislation to tackle the conduct. The problem I would say is that the conduct by its nature, makes it difficult to identify the suspect as he is usually anonymous hiding behind the virtual cyber world. Sometimes, the victims may not even realize that they are victims”.

Likewise, PRO25 emphasised that there is “no specific legislation for cyberstalking”.

Additionally, PRO25 stressed that in some cases cyberstalkers are not prosecuted because they had not yet “made threats of violence”. PO25 however did not explain if this is because victims delay in reporting incidents until cyberstalkers make threats of violence. PRO25 also, echoed the frustration of the participants regarding the perceived inadequate sentencing powers of the magistrate’s courts;

PRO25: “My general view is that there are too many legislations on harassment and no specific legislation on cyberstalking. In some cases, the cyberstalker commits several years of the offence but because he has not made threats to violence, he is not prosecuted. Also, the sentencing powers of the magistrates is limited to 6 months. People questioned why a cyberstalker in a case that I dealt with wasn’t in the crown court. The cyberstalker in this case had 60 years of no previous conviction, he got 1 week off for pleading guilty and was sentenced to only 6 months. Compared to other offences that go to the crown court, an extended cyberstalking over a lot of years has more effect on the victim. Greater sentencing power is required to cover it”.

216
In contrast to the above views, some of the participants expressed the view that the existing laws are effective. Particularly, the participants who held this view, said “the laws are very good because restraining orders can be imposed under existing legislation to prevent convicted cyberstalkers from contacting victims further” (PO14).

Int: How effective do you think that the laws in this country are against cyberstalking?

PO14: “I think that they are very good”.

Sub Question: In your opinion why do you think that the laws are very good?

PO14: “When the cyberstalkers are charged and they go to court, when they are convicted, there is a restraining order that can be imposed under existing legislation to prevent cyberstalkers from contacting victims further”.

Like PO14, PRO2 shared the perception that the laws are adequate:

PRO2: “I think that the laws are adequate. Particularly the restraining order aspect of them”.

Like PO14 and PRO2, PRO9 also shared the perception that the current legislation offers victims the opportunity to apply for restraining orders;

PRO9: “The good thing about the act is that it gives the victim the opportunity to apply for a restraining order to protect her from future harassments”.

Like PO14, PRO2 and PRO9, PO30 also shared the perception that existing laws are effective because they enable prosecutors to apply for restraining orders especially in cases involving repeat offenders. PO30 therefore, explained that a judge in a case
that he reviewed, “imposed a restraining order after a cyberstalker was successfully convicted because the cyberstalker had previous records”.

However, from a critical perspective, PRO22 said that in some cases, offenders “lodge civil action claims to circumvent the restraining orders that have been imposed by judges”. It is important to note that the participants did not share PRO22’s view which is highlighted in the extract below.

Int: Briefly outline your experience to date with law enforcement to do with cyberstalking?

PRO22: “I investigated a case in which a cyberstalker was convicted and the court granted a restraining order against him to prevent him contacting the victim. The defendant then lodged a civil claim action in order to circumvent the restraining order. The defendant claimed that his human rights had been breached. The question was how had his human rights been breached by the issue of the restraining order?”

Sub Question: What was the outcome of the case?

PRO22: “It was a significant case. Until this case, no one realized that a cyberstalker could use civil law to circumvent prohibitions or restraining orders not to communicate with or contact victims”.

Similarly, PRO5 expressed frustration at the ability of convicted cyberstalkers to persist in harassing victim after breaching restraining orders;

PRO5: “I have the experience of reviewing a case which involved an element of cyberstalking. In this case, the cyberstalker and the victim were in a relationship. The cyberstalker committed further offences after breaking a restraining order not to contact the victim. The officer in this case was infuriated because it demonstrated how ineffective restraining orders can be at times in protecting victims”.

218
A minority of the participants expressed frustration at the high burden of proof. Although they did not elaborate on what they meant, PO18’s extract served to further affirm this view.

Int: What, in your opinion, are the issues with definition of cyberstalking that need to be addressed?

PO18: “The definition of stalking and the burden of proof should be made easier so that the conduct can be proven in court because we have to look at it from the victim’s point of view. The burden of proof is too high and it may be challenge to proof a course of conduct or an offence under s4 of the PHA”.

The participants emphasised that an issue which frustrates them is that it may be difficult to proof that a cyberstalker’s behaviour amounted to a course of conduct as defined under S7 of the PHA. Consequently PRO26 echoed the frustration of the participants and reiterated that the PHA requires a conduct to have occurred on 2 consecutive occasions as opposed to isolated incidents.

Int: What in your opinion are the issues with the definition of cyberstalking that need to be addressed?

PRO26: “For me it has to be clear looking at a cause of conduct over a number of occasions. The law states that you need a cause of conduct on two occasions. If you have a cause of conduct with five elements, you will have a strong case as opposed to isolated incidents. You need to have strong evidence and understand the legislation. For example, if someone sends an offensive text message on 1/1/13 and another after 6 months, it is the last incident that will be charged. If I put a wreath on a neighbour’s door on 1/1/14 every year, it is the last one within the last 6 months that will be considered. So it may be difficult to prove a cyberstalker’s behaviour amounts to a course of conduct under the PHA if the incidents are isolated and not consecutive”.

219
The participants also expressed their frustration at the statutory time limit for bringing offences under the PHA which they perceived to be short. Hence, PRO17’s in his extract, echoed the views of many of the participants;

PRO17: “The legislation should be amended to give lawyers more time to prosecute. For the S4 offences under the Protection from Harassment Act, there should be no time limit for establishing the offence of putting a person in fear of violence once it can be shown that an electronic communication has been made and that the communication contained elements of cyberstalking. The summary only offence under S2 of the act carries a sentence of 6 months imprisonment”.

Like PRO17, PRO23 discussed perceived issues with the statutory time limit under the PHA. PRO23 was frustrated by the fact that some victims report cases after the six months statutory time limit for initiating legal proceedings. PRO23 explained the reasons for his frustration in his extract;

PRO23: “The laws are ok in my view. My issue is that we cannot investigate and prosecute cases which are reported out of time. This situation results in offenders not being prosecuted. This leaves them free to continue offending. The reason is because, in summary only offences, there is a legal requirement for complaints to be commenced within 6 months from the time when an offence was committed, or the matter of complaint arose. It is exasperating for police officers when cyberstalkers cannot be prosecuted because victims have made formal complaints of harassment against cyberstalkers six months after the incident complained of”.

While discussing the effectiveness of the existing legislation, many of the participants shared the perception that it was difficult to gauge the effectiveness of existing legislation because some victims do not report incidents. The participants stated that it was frustrating when cyberstalkers are not investigated and prosecuted because victims fail to report incidents formally. Therefore the participants attributed the issue of under reporting to various factors. The factors were; “fear of getting involved with
the police”, (PO7), “lack of confidence in the criminal justice system” (PO11), “victims thinking that cyberstalking is not a serious offence” (PO21) and “victims deciding to rekindle relationships with offenders in domestic violence cases” (PO14). PO7’s extract, illustrates the frustrations of the participants. Particularly, PO7 stressed that there will be “missed opportunities” to prosecute offenders if victims do not report incidents to the police;

PO7: “At the moment, there is a fear of getting involved in the police or the criminal justice system. It is difficult to say if the fear is justified. My only worry is that if victims do not report cyberstalking incidents to the police, it will lead to missed opportunities for prosecutors to charge offenders”.

Some of the participants emphasised that the effectiveness of existing legislation cannot be assessed due to several reasons. Hence they remarked “stalking offences are recorded as harassment” (PO7), “some victims are reluctant to report offences” (PRO11) “not every single incident is investigated” (PO14) and “cyberstalking is not deemed a serious offence” (PO20).

Similarly, a minority of the participants discussed the perceived preferential treatment that celebrity victims will receive in cases involving the extradition of cyberstalkers. The participants shared the perception that cyberstalkers who stalk from abroad and target non-celebrities will not be extradited because, cyberstalking is not deemed to be a serious enough offence that warrants the extradition of an offender. The participants discussed the difficulties of extraditing cyberstalkers in other jurisdictions because they wanted to highlight there was also a jurisdictional difficulty to the investigation of cyberstalkers given that there is no geographical barrier to
cyberstalking. The jurisdictional difficulties are discussed in Chapter 1, section 1.1. PO6’s extract, reflects the views of the participants.

Int: What are the existing extradition arrangements specifically relating to cyberstalking?

PO6: “There is no chance of a cyberstalker being extradited. No chance at all”.

Sub Question: In your opinion, why do you think that there is no chance of a cyberstalker being extradited?

PO6: “The offence is not considered serious enough to warrant the extradition of a cyberstalker”.

Sub Question: In your opinion if the cyberstalker threatens to kill the victim will the offence be considered serious enough to justify the extradition if a cyberstalker?

PO6: “We will have to convince the CPS and the law enforcement officials that the offence is serious. The problem is that it is not that simple or easy to warrant the extradition of a cyberstalker. If the case involves a celebrity it is media worthy and will be viewed to be in the public interest and vice versa”.

Like PO2 and PO6, PRO17 expressed frustration at the perceived preferential treatment that is given to victims who are in the public eye. Notably, PRO17’s extract made specific reference to 2 politicians who were victimised by cyberstalkers.

Int: What in your opinion are the issues with definition of cyberstalking that need to be addressed?

PRO17: “Celebrity cases generate media publicity such as the cases of Stella Creasey and Caroline Criado Perez who are members of parliament who were recently cyberstalked. I wish cases involving ordinary members of the public especially in domestic violence cases, generated the same publicity to increase public awareness on the issue”.
Given that cyberstalking is committed in the virtual realm, a minority of the participants were doubtful that cyberstalkers will be deterred by existing legislation. Therefore, P025 remarked in his extract, “You can’t stop the offence with regulation”.

PRO25: “You can’t stop the offence with regulation. The answer to the question is that you can regulate the offence but you cannot control the behaviour. So the legislation can never be sufficient”.

In conclusion the participants shared the perception that several legislative issues frustrate them in the investigation and prosecution of cyberstalkers. The frustration ranged from the perceived issue of lenient sentencing to the perceived proving offences under the PHA.

4.3.3 Theme 3: Lack of training and knowledge

Lack of knowledge and training’ was the third main theme that emerged from the interview data. In total, 88% out of 100% of the police officers and 80% out of 100% of the prosecutors, highlighted the areas of knowledge that were lacking. Additionally the participants shared the perception that they require training in several areas. The areas include retrieving, assessing and preserving electronic evidence, risk assessment, legislation and connecting cyberstalkers to unregistered SIM cards.

The data presented in Table 4.7 below indicate that the sample of police officers lack knowledge in 8 areas and that the sample of prosecutors lack knowledge in 5 areas. The data presented in Table 4.8 below indicates that the sample of police officers require training in 11 areas and that the sample of prosecutors require training in 5 areas.
The participants discussed the measures they have adopted to acquire the gap in their professional knowledge. The wide ranging measures are highlighted in Tables 4.9 and 4.10. The police officers identified 6 self-help measures that they have adopted to acquire the knowledge they lack in comparison to the prosecutors who identified 10 self-help measures.

Table 4.7: Self-perceived areas in which police officers and prosecutors identify lack of knowledge when investigating and prosecuting cyberstalkers

<table>
<thead>
<tr>
<th>Lack of knowledge</th>
<th>Number of police officers</th>
<th>Percentage of sample</th>
<th>Number of prosecutors</th>
<th>Percentage of sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risking assessing suspects on arrest who have no obvious signs of mental illness</td>
<td>2</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Identifying cyberstalkers who may need to be risk assessed</td>
<td>2</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unmasking the identities of cyberstalkers who use dongles to victimise</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Connecting cyberstalkers to unregistered SIM cards</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Connecting cyberstalkers to unregistered SIM cards</td>
<td>3</td>
<td>12</td>
<td>3</td>
<td>10</td>
</tr>
</tbody>
</table>
Table 4.7 Self-perceived areas in which police officers and prosecutors identify lack of knowledge when investigating and prosecuting cyberstalkers

<table>
<thead>
<tr>
<th>Lack of knowledge</th>
<th>Number of police officers</th>
<th>Percentage of sample</th>
<th>Number of prosecutors</th>
<th>Percentage of sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stalking laws</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Tracking cyberstalkers</td>
<td>5</td>
<td>20</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>ISP strategies for combating cyberstalking</td>
<td>7</td>
<td>28</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>Unmasking anonymous cyberstalkers</td>
<td>3</td>
<td>12</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Lack of police knowledge on CPS evidential threshold</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of police knowledge on the rationale for providing</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>further evidence after charge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>24</td>
<td>96</td>
<td>28</td>
<td>93</td>
</tr>
</tbody>
</table>
Table 4.8: Self-perceived areas in which police officers and prosecutors identify lack of training when investigating and prosecuting cyberstalkers

<table>
<thead>
<tr>
<th>Lack of training</th>
<th>Number of police officers</th>
<th>Percentage of sample</th>
<th>Number of prosecutors</th>
<th>Percentage of prosecutor sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracing email and IP addresses</td>
<td>4</td>
<td>16</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Phone and computer evidence</td>
<td>4</td>
<td>16</td>
<td>9</td>
<td>30</td>
</tr>
<tr>
<td>Computer forensics</td>
<td>2</td>
<td>8</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>Obtaining digital evidence</td>
<td>3</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Accessing digital evidence</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Preserving digital evidence</td>
<td>3</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Judicial training</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Identifying digital evidence</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Psychological impact of Cyberstalking</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>13</td>
</tr>
</tbody>
</table>
Table 4.8: Self-perceived areas in which police officers and prosecutors identify lack of training when investigating and prosecuting cyberstalkers

<table>
<thead>
<tr>
<th>Lack of training</th>
<th>Number of police officers</th>
<th>Percentage of police sample</th>
<th>Number of prosecutors</th>
<th>Percentage of prosecutor sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most effective way of gathering evidence</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Risk assessment of offenders</td>
<td>3</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Risk assessment of victims</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>25</td>
<td>100</td>
<td>25</td>
<td>83</td>
</tr>
</tbody>
</table>
Table 4.9: Perceptions of the police officers on the self-help measures that they adopt to close the knowledge gap

<table>
<thead>
<tr>
<th>Perceptions of police officers on self-help measures that close the knowledge gap</th>
<th>Number of police officers</th>
<th>Percentage of sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask experienced colleagues within the department</td>
<td>14</td>
<td>56</td>
</tr>
<tr>
<td>Acquire knowledge during the investigation process</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>Personal research on how to trace anonymous internet portal and email addresses</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Read the malicious communications guidance</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Liaise with specialist police officers who are based in the Police Central e-Crime Unit</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Liaise with colleagues in other departments</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Total</td>
<td>25</td>
<td>100</td>
</tr>
</tbody>
</table>
Table 10: Perceptions of prosecutors on the self-help measures that they adopt to close the knowledge gap

<table>
<thead>
<tr>
<th>Perceptions of prosecutors on self - help measures that close the knowledge gap</th>
<th>Number of prosecutors</th>
<th>Percentage of sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal sources such as Archbold, Blackstone, and Westlaw</td>
<td>9</td>
<td>30</td>
</tr>
<tr>
<td>Liaise with experienced colleagues</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>CPS Guidance</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>CPS Info net</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Creation of spreadsheet of cases for personal knowledge</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Law books</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Legislation</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Online library</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Personal research</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Reading case reviews</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>30</td>
<td>100</td>
</tr>
</tbody>
</table>

The participants talked about missed opportunities to risk assess cyberstalkers who do not display any obvious signs of mental illness when arrested. Hence, PO12 in his extract, reflected the frustration of the participants;

PO12: “Sometimes, we arrest suspects who have mental health issues. I feel that an issue is that police officers in some cases may be unaware that an offender is mentally ill. This can lead to missed opportunities. The reason is because due to lack of knowledge, it is difficult to risk assess cyberstalkers who have no obvious signs of mental illness”.

Like PO12, PO15 while discussing the difficulties that police officers face in the prosecution of cyberstalkers, revealed that it is difficult to “spot the hidden symptoms”
Hence PO15 said in his extract that police officers lack specialist knowledge on how to identify offenders who are mentally ill;

PO25: “A problem is identifying cyberstalkers who have mental health issues. It is an issue because, it is not always apparent that they require medical assistance. We will benefit from training on how to spot the hidden symptoms on arrest”.

The participants expressed frustration at not being able to trace anonymous cyberstalkers. While the participants shared the perception that there is the danger of anonymous cyberstalkers evading justice, PO14 indicated that he lacked knowledge on how to unveil the identity of customers who use dongles to victimise. PO14 in his extract explained why he was frustrated by the issue;

PO14: “Although a cyberstalker can obtain 3 dongles for a laptop some ISPs, are still unable to link the users of dongles to the relevant internet subscriptions. ISPs use the knowledge gap as an excuse for not being able to disclose the internet details of suspects to police officers”.

Like PO14, PRO1 discussed how lack of knowledge impedes the investigation process. Hence, PRO1 stated that he lacked knowledge on how to connect cyberstalkers to unregistered subscriber identification module (SIM) cards. Notably, PRO1 indicated that lack of knowledge and evidential difficulties can lead to cases being dropped;

PRO1: “I once investigated a case which involved a news reader who was being cyberstalked. During the course of the investigation, we faced some obstacles. First, the cyberstalker was using an unregistered telephone so it was impossible to trace the call or identify the culprit. Next the internet service providers were not willing to help. We stopped investigating the case because we could not prove it without the telephone evidence”.

230
When asked how effective they considered the laws in the UK against cyberstalking to be, some of the participants said “We do not know much about it” (PO8). Likewise, the participants talked about lack of experience and said “The problem is that the police need technical experience to investigate cases” (PO13). Hence, PO10 suggested that police officers require training on the implementation of existing legislation. PO10’s extract, demonstrates this;

PO10: “I think that the current legislation is effective - what we need is training on how to implement the amended PHA and existing legislation. The training will provide the knowledge required on how to apply legislation to cases”.

While discussing the difficulties that police officers face in the prosecution of cyberstalkers, the participants expressed their frustration at the perceived “knowledge gap” among the ISPs, judiciary, CPS and the police. PO22’s extract reveals the frustration of the participants that the ISPs do not have the knowledge required to unmask the identity of anonymous cyberstalkers.

PO22: “There is also a knowledge gap among the judiciary which has led to a problem with presenting the technical aspects of such a case. For example, when I approach judges for productions orders to access the IP addresses, email addresses, and so on of cyberstalkers, they turn around and ask for help on how to protect themselves online. This knowledge gap is a big problem - the judiciary, defence, and the prosecutors all need to be trained in my view”.

The participants shared the common frustration that there is a lack of knowledge among members of the public on the psychological impact of cyberstalking on victims and also a lack of knowledge among the judiciary which may affect how judges direct jurors during trials. Echoing this view, PRO16 explained that there was a dangerous
misconception that because cyberstalking is not a physical offence, victims are affected less seriously;

PRO10: “The final point that I will like to raise is that research has to be undertaken to increase the public and judicial awareness of the psychological harm that is done to victims. Research is required to assess the level of impact on the victim to assist the prosecutors in the building of cases. The courts in general have difficulties in explaining cyberstalking to the jurors because there is a perception that cyberstalking constitutes a virtual offence and not an immediate physical threat. This is a wrong and dangerous perception to have. A lot of people feel that if there is no physical harm, then no serious damage has been done. They don’t realize that they can cause devastating harm to the victim by damaging their reputation through libellous comments and psychologically through mental damage. There is therefore, a lack of knowledge on the impact of cyberstalking on victims”.

The participants also expressed frustration at the lack of police knowledge on the CPS evidential threshold and the rationale for providing outstanding evidence after defendants have been charged. The tone of PRO27’s extract, reflects the frustration of the participants;

PRO27: “Another difficulty is that some police officers have to be repeatedly enlightened by prosecutors on the CPS evidential threshold and how we arrive at charging decisions. This results in us having to repeatedly request outstanding evidence while explaining again, we require the evidence. They do not seem to realize that we cannot progress cases until they provide sufficient evidence to prove that there is a realistic prospect of convicting an offender”.

While discussing how lack of knowledge hinders police officers from investigating cyberstalkers, PRO13 expressed the view that an investigative issue which frustrates him is the lack of evidential clarity on the best way to gather evidence from the internet. PRO13 equally shared the perception that the participants faced challenges in trying to trace electronic evidence;
PRO13: “There is lack of evidential clarity on the best way to gather evidence from the internet. Another issue that I can think of is the difficulty in identifying the defendant. There is the difficulty of tracking where the communication is coming from”.

When asked if they had received training on the investigation of cyberstalkers, the participants shared the perception that police officers lacked the requisite knowledge on how to trace the emails or internet portal addresses of suspects.

PO19’s extract highlights the frustration of police officers in having to obtain knowledge from the internet on how to trace the email and IP addresses of suspects rather than being trained how to do this;

Int: Have you received any training on cyberstalking?

PO19: “I have not received any training on how to investigate the conduct of cyberstalking”.

Sub Question: Where have you obtained the knowledge that you so far have on the subject from?

PO19: “I have obtained it from the internet. That is tips on how to investigate or trace the email addresses and IP addresses of suspects. I have obtained my knowledge from the internet”.

While discussing how lack of knowledge and training can impact on how police officers investigate cyberstalkers, PO21 in common with PO19 revealed that police officers had not received the required training. PO9’s extract shows the frustration of the participants;
Int: Have you received any training on cyberstalking?

PO21: “At the moment we have received no training. We have not been trained on phone and computer crimes. We have not received the computer forensic police training required to investigate such a digital crime”.

However, PO21’s extract below reveals that there is an assumption that police officers will acquire knowledge on how to investigate cyberstalking cases during the investigation process;

Sub Question: Where do you obtain knowledge of the conduct from?

PO21: “From the officers in my team who have investigated such cases or similar cases. This is one of those offences where you are required to learn about the offence as you are investigating it. You will probably get to learn more about the offence or have a decent idea about what it is about by the end of the investigation”.

While discussing cyberstalkers who use encrypted messages and fake email addresses to target victims, the participants expressed frustration at the lack of knowledge on how to access encrypted messages. Hence, PO24 makes it clear that all police require training in general on the investigation of cyberstalkers;

PO24: “Finally, the police officers have not been given the required training needed to effectively investigate the crime. This ranges from the lowly paid police officers to the most senior police officers. There is an urgent need for such training given the rapid technological advancement”.

When asked the difficulties that police officers face in the prosecution of cyberstalkers, the participants shared the perception that police officers lack specialist knowledge on how to access and preserve electronic evidence at the time of the study;
PO17: “The police should also be trained on how to access preserve digital evidence which is crucial to building strong cases against cyberstalkers. Not all police officers have received the training”.

Similarly, the participants shared the perception that only specialist police officers have the requisite knowledge for investigating cyberstalking cases. PRO16’s extract reinforces this view. Notably, PRO16’s comments revealed that lack of specialist knowledge can result in cases being dropped if police officers cannot retrieve the evidence required to prosecute offenders;

PRO16: “Firstly, the police do not understand it. They have a special crime department which is supposed to specialize in electronic, media and telephone. They state that deleted emails and texts can be retrieved. The specialist officers know this but ordinary police officers don’t as they can’t help you when the victim claims that the offensive messages have been deleted. Cases can get dropped if the police officer does not have the knowledge or if a victim for example drops her phone in the bath and losses relevant evidence”.

The above observations highlight the shared perceptions of the police officers and prosecutors on the issue of lack of training and knowledge and are based on perceived difficulties in relation to various areas. The data in Table 4.7 indicates that the police officers identified 8 areas of knowledge that were lacking and that the prosecutors identified 6 areas of knowledge that were lacking therefore this adds weight to their assertions that all involved in investigating and prosecuting these crimes receive appropriate, sufficient and current training.

Most of the participants highlighted lack of training as an issue which frustrates them in the investigation and prosecution of cyberstalkers. Therefore, the participants stated that they had not received “specific training” (PO3), “any training” (PO2, PO4 and
PO5), “special training outside the normal detective training” (PO15), “training on how to investigate the conduct” (POI6) and “training on the technological aspects of the case” (PO25).

PO11 expressed the view that he had received “no training because cyberstalking is part of general policing”. Consequently, in justifying why participants had resorted to self-help measures to obtain the lacking knowledge, PO4 remarked “we have received no training and so we all grab help from where we can….in the beginning, cyberstalking was an unknown conduct and so, liaising with other relevant officials is crucial”.

Worryingly, PO6 remarked “no training is required if you have the required evidence because “cyberstalking is another form of harassment and public disorder”. It is also concerning that PO12 remarked “no training has been offered to me. I do not think that the MET realizes cyberstalking is becoming a growing concern”. Likewise, PRO4 endorsed the views of many of the participants by stating a problem which will hinder the prosecution of cyberstalkers in that “there are not enough trained law enforcement officials”.

From a governmental perspective, MEP remarked “there are not enough trained police officers to investigate the conduct”. In contrast, PO24 was optimistic that training will be provided in the future and remarked “I anticipate that training will be provided in the future”. 
Notably, the tone of PO5’s extract highlighted his frustration that he had not been trained on how to investigate cyberstalkers. Hence, he suggested that “all police officers should be offered training”;

Int: Have you received any training on cyberstalking?

PO5: “No. I have not received any training. What I know, I learnt on the job. In my view all police officers should be offered training to equip them with the skills required to investigate the conduct”.

It is important to note that some of the participants revealed that they had received training on harassment in general although they had not received specific training on cyberstalking. Of concern is the fact that POI8’s extract demonstrates that it was not clear to some participants whether harassment and cyberstalking are offences investigated under the same category of offences;

PO18: “I have not received any training for cyberstalking although I have received training for harassment. It falls under the same category doesn’t it?”

Like PO5, PO9, PO12, and PO15 respectively, PO21 remarked “I have learnt about the offence on the job.” PO21’s extract reiterated that the majority of the participants have not received any training and have resorted to self-help measures to obtain the requisite knowledge:

Int: Have you received any training on cyberstalking?

PO21: “I have not received any training relating to cyberstalking. The little knowledge that I have is derived from materials that I have read online during
my own spare time. I have not received any formal training. I have learnt about the offence while investigating cases. I do not believe that there is any specialist police training that is being given for cyberstalking cases.

From a positive perspective, some of the police officers indicated that they had received “normal 5 week training on harassment and a 1 day domestic violence course” when they were first recruited (PO13), training on the “Computer Misuse Act” (PO7), “nothing outside the normal detective training” (PO9), “on obtaining mobile phone evidence as part of the detective course” (PO14) and “training on harassment as part of the detective course” (PO18). Notably, PO13 in her extract stated that she had received an additional 1 day in domestic violence training which implicitly, provided additional training on harassment arguably in relation to domestic violence cases.

Int: Question: Have you received training on cyberstalking?

PO1: “No. I have not received any specific training. I had the normal 5 weeks training at Hendon. I did the one day domestic violence course which was because I was working on the domestic violence unit then. This enabled me to learn what harassment was and revisit the law”.

Like PO13, PO19 indicated that he had received training “on how to do a lot with mobile phones”. PO19 highlighted that the training educated him on how to connect telephone cell cite maps to an address;

PO19: “I have taken part on a detective training course as I was explaining how you can do a lot with a mobile phone. It was useful as it enlightened me on how mobile phones can be linked to a crime scene. We can then link the cell cite map to an address”.

Additionally, some of the prosecutors confirmed that they had received “online training” at the time of the study (PRO7, PRO11, PRO18). Another participant highlighted that
she was given useful “hand-outs” on cyberstalking by her manager (PRO3). Further, participants indicated that they had received training from a “pupil master” (PRO12) and had “completed an e-learning cyberstalking module” (PRO13).

Notably, PRO15’s extract reflected the view of the participants who were optimistic that more training will be provided in the future;

PRO15: “I have received some training. Training will be more developed in the future I hope. We have the new prosecutor’s guidelines for prosecuting cases involving the sending of malicious tweets”.

Many of the participants expressed PO8’s view “that the investigation process is a “learning experience on how to investigate digital crimes”. The participants therefore, explained how they obtain knowledge given that the relevant training had not been provided at the time of the study. Hence, PO15 said “what we know we learnt on the job” and PO6 remarked that he gained knowledge “during the course of the investigation’. Also, the participants stated that they obtained knowledge “from the internet” (PO9), from experienced colleagues in my team” (PO10) and “learnt while investigating cases” (PO11). Similarly, PO12 explained that he acquired knowledge by “referring to the standard operating guidance”. PO15 shared PO12’s view by stating that he gained knowledge by “asking experienced Colleagues questions”.

Additionally, the tone of PO19’s extract, echoes the views of PO5, PO6, PO12, PO15 and PO21 who perceive investigation processes as learning processes;

PO19: “I have not received any training on cyberstalking. I have obtained the limited knowledge that I have from doing the job. When I first investigated a cyberstalking case, I had to ask my colleague for help as I had received no
training whatsoever. In other words, I relied on colleagues who had a lot of experience”.

In conclusion, the above observations highlight the shared perceptions of the participants on how lack of knowledge and training, hinder police officers and prosecutors from bringing cyberstalkers to justice. The data in Table 4.7 attests to this and furthermore, Table 4.8 indicates that the sample of police officers recognise that they require training in 11 areas and the sample of prosecutors require training in 5 areas.

4.3.4 Theme 4: Lack of resources

‘Lack of resources’ was the fourth main theme identified from the interview data. Importantly, all of the police officers and 97% of the sample of prosecutors shared the perception that lack of resources was a factor that frustrates police officers in the investigation and prosecution of cyberstalkers. The participants highlighted six perceived aspects which frustrate them namely, missed opportunities to risk assess victims and offenders, inability to risk manage victims, managing heavy caseloads, inability to meet CPS deadlines, shortage of staff and inability to fulfil the public expectation that police officers will investigate every cyberstalking incident.

The prosecutors and police officers highlighted 8 and 6 perceived lack of resources respectively which they report frustrate them in the investigation and prosecution of cyberstalkers. The perceived legislative issues are presented in Table 4.11.
Table 4.11: Perceptions of police officers and prosecutors on lack of resources:

<table>
<thead>
<tr>
<th>Perceptions of prosecutors on lack of resources</th>
<th>Number of police officers</th>
<th>Percentage of sample</th>
<th>Number of prosecutors</th>
<th>Percentage of prosecutors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missed opportunities to risk assess victims</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Unable to manage risks to victims</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unable to risk assess cyberstalkers</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Insufficient specialist and non-specialist staff</td>
<td>4</td>
<td>16</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Retention of staff</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Excessive caseloads</td>
<td>4</td>
<td>16</td>
<td>6</td>
<td>17</td>
</tr>
<tr>
<td>Inability to meet CPS deadlines for providing evidence</td>
<td>3</td>
<td>12</td>
<td>6</td>
<td>17</td>
</tr>
<tr>
<td>Unrealistic public expectation to investigate all cyberstalking cases</td>
<td>3</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Insufficient time to follow up on initial reports by victims</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Lack of centralized database for sharing local intelligence</td>
<td>3</td>
<td>12</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Lack of a single point of contact</td>
<td>2</td>
<td>8</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>Frequency</td>
<td>25</td>
<td>100</td>
<td>26</td>
<td>83</td>
</tr>
</tbody>
</table>
While discussing the risk assessment of victims, the participants shared the perception that shortage of manpower can lead police officers not being able to “manage the risks to victims”. PO1’s extract echoed the frustrations of the participants concerning this;

PO1: “The laws are effective especially the amended PHA. The problem is trying to manage the risk to victims once a cyberstalker has been identified due to lack of resources”.

The participants also expressed frustration at how the shortage of manpower can lead to police officers failing to realize that offenders may be suffering from mental illnesses. Consequently, PO3 expressed frustration at how lack of resources hinders police officers from carrying out risk assessment measures. However unlike PO1, PO3 expressed his frustration regarding the inability of police officers to risk assess cyberstalkers as opposed to victims. Particularly, PO3 highlighted a case involving a mentally ill cyberstalker who was not risk assessed due to staff shortage. Hence, PO3 remarked that staff shortage can result in a police officer “misjudging situations when a cyberstalker needs to be risk assessed”. Notably, PO3 highlighted that in some cases, cyberstalkers may require “counselling and support”;

PO3: “I think that the laws are fine. The problem is insufficient resources. I dealt with a bloke who rented a flat opposite a bar after developing an obsession with a bar maid. In the beginning, he went into the bar and frequently struck up conversation with the barmaid then it progresses to him buying presents and then turning up frequently at her work place. The stalker was arrested and put in custody. During investigation, it later came out that the defendant was suffering from a mental illness which obviously affected his judgement. The scary thing is that this case had previously been investigated by a colleague who just believed that the stalker had an unhealthy interest in the victim. The shortage of manpower led to my colleague misjudging a situation when a cyberstalker need to be risk assessed on arrest. The bigger picture is that a cyberstalker may need counselling and support”.

242
Likewise, PRO19 discussed how due to staff shortage, police officers may not recognize when mentally ill cyberstalkers require medical assistance. However, PRO19 queried why “people assume that all cyberstalkers are sane”. “PRO19’s extract supported PO3’s views.

PRO19: “The existing legislation offers victims the opportunity to apply for a restraining order. My concern is that if a mentally ill cyberstalker who targets victims in the physical and cyber realms is arrested, an over-worked arresting police officer may fail to risk assess the offender and recognize that the offender is suffering from a mental illness and therefore requires medical assistance. Why do people assume that all cyberstalkers are sane?”

Likewise, PRO30 explained that the due to the shortage of trained specialist and non-specialist staff, police officers investigating cases may fail to recognize the “warning signs” that a domestic violence victim is also being cyberstalked by her former partner. PRO30 perceived the warning signs to include former partners sending victims obscene, intimidating and threatening emails. PO30 stated that the warning signs also include victims receiving persistent unwanted telephone calls from cyberstalkers

Likewise, the tone of PO4’s extract, strongly echoed the frustration of the police officers at the shortage of manpower hindering police officers from risk assessing victims. Hence, PO4 indicated in his last sentence that he was unable to risk assess an anonymous cyberstalker;

PO4: “I think you have cyberstalking cases where the defendant is not known that is what comes to mind. I investigated a cyberstalking case where the identity of the cyberstalker was not known to the police due to the anonymous nature of the offence. As a result, it was impossible to monitor the cyberstalker or to carry out an effective risk assessment”.

243
The police officers were frustrated by the perceived public expectation that every single cyberstalking incident that has taken place will be investigated. Hence PO22 remarked that that the perceived public expectation is unrealistic because police officers cannot investigate every single case”. PO22’s extract reiterated the view of PO14 that police officers “cannot investigate every single incident”;

PO22: “If you speak to the victims they will say the laws are not effective because the conduct is not taken seriously. There is I suppose, a public expectation that police officers will investigate all cyberstalking cases. The public expectation in my view is unrealistic because we cannot investigate every single case. The victims I suspect feel let down because high profile celebrities are protected more by the legislation than ordinary members of the public. Then again should the police investigate every single complaint by a member of the public?”

The participants linked the issue of lack of resources to the allocation of heavy caseloads. In doing so they expressed further frustration that the allocation of heavy caseloads “leads to police officers being overworked” (PRO5), “puts police officers under enormous pressure” (PO12) “creates the problem of staff retention” (PO18) and “delays the time that it takes for police officers to complete investigative actions” (PO24). PRO5 echoed the views of the participants and said that it is challenging for police officers to provide outstanding evidence within strict deadlines because they are “juggling the investigation of several cases due to having heavy caseloads”.

Int.: In your opinion do you think that police officers are allocated too many cases and if so why?

PRO5: “Although I am not a police officer, I work with police officers daily and some of them have made it known in the past that they are overworked which is why they have been unable to provide the evidence within stipulated deadlines that the CPS requires to prosecute certain criminals. Some of the police officers also complain that there is a staff shortage and a high expectation for them to complete investigations within strict deadlines. The
situation can become exasperating for prosecutors too when we are dealing with several cases including cyberstalking which might require us to risk assess victims. I would say that the exasperation felt by some police officers has an inevitable impact on their ability to provide the evidence required by prosecutors to build robust cases against criminals. They are overworked and are juggling with the investigation of several cases due to having heavy caseloads”.

PO24 echoed the frustrations of PRO5 on the challenges faced by police officers to provide evidence due to lack of resources. However, PO24 highlighted that this issue leads to judges giving court directions for the CPS to provide outstanding evidence within strict court deadlines;

PRO5: “What I do know is that lack of manpower is having a negative impact on the ability of police officers to provide outstanding evidence and the prospect of prosecutors to build robust cases. This evidential delay in proving evidence leads to judges orders. The orders require the CPS within strict deadlines”.

Likewise, PRO6’s extracts support the views of PRO5 and PO24. The extract reveals that the participants were frustrated because, they are unable to meet CPS deadlines due to lack of delay;

PRO6: “Staff shortage can prevent police officers from following up on initial reports by victims within stipulated CPS deadlines due to the fact that police officers are investigating serious and complex cases with the investigation of cyberstalking cases.

Similarly, PRO11 expressed the view that due to staff shortages, police officers do not promptly provide outstanding evidence requested by the prosecution which can be frustrating for prosecutors:

PO11: “A police officer who I work with regularly once told me that the reason why some police officers do not provide evidence that the CPS requires within specific deadlines is because they are investigating several cases
simultaneously. The police officer stated that the work overload delays them from proving outstanding evidence promptly because they are tasked with investigating several cases at the same time. This situation prevents prosecutors from building strong cases against cyberstalkers due to lack of evidence because we have to ensure that cases meet the evidential threshold”.

While discussing the difficulties that police face in the prosecution of cyberstalkers PRO11 like PO24, shared the perception that staff shortage was an investigative issue. However, PO24 referred specifically to the lack of computer experts in addition to ordinary police officers. The tone of PO24’s extract, highlighted his frustration which is reflected in the last sentence of his extract in which he describes the issue as “an investigative predicament”;

PO24: “We do not have enough computer experts to investigate the cases given the expansion of information technology. In addition, we also lack ordinary police officers. This is an investigative predicament”.

Notably, while discussing the effectiveness of existing laws in this country against cyberstalking, the participants shared the perception that lack of resources can lead to police officers not taking initial allegations seriously and not adequately implementing the laws adequately. Hence, PO25 linked the perceived issue of inadequate implementation of existing legislation to heavy caseload. PO25’s extract was representative of the views of most of the participants;

PO25: “The legislation is ok because I think that it is sufficient. The problem we face is that there is the danger of police officers not taking initial allegations seriously due to a heavy caseloads thereby not implementing the legislation as and when required”.

It is important to note that the some of the participants revealed that due to lack of resources, sometimes police officers may not deem cyberstalking to be a serious
offence in comparison to other offences if they are required to prioritise cases. Hence PO18 in his extract, referred to cyberstalking as a “minor offence”;

PO18: “The difficulty that springs to mind is shortage of manpower which makes us prioritise cases more. When cases are prioritised, the investigation of rape, murder or kidnap cases may take priority over the investigation of a cyberstalking case. Having said that, it all depends on the facts of a case”.

Like PO18, PO23 expressed the view that cyberstalking is not deemed serious enough. However, PO23 highlighted that due to lack of resources, police officers will have to justify spending “limited resources” on a cyberstalking case instead of “other major crimes”. PO23’s extract revealed the frustration of the participants;

PO23: “The reality is that the police want to help in the investigation of cyberstalking but officers will have to justify the merit of investigating such a conduct. They will have to explain why the limited resources should be employed and why the case should be prioritised over other major crimes. In the UK, cybercrime is classified as a Tier 1 threat meaning that it is very serious given the implication with international terrorism. However, when you start comparing it to rape, murder and so on, it becomes an issue for the police officers who may have different views given the problem of limited resources”.

While discussing the problems that police officers face in the prosecution of cyberstalkers, the participants also discussed the issue of lack of designated cyberstalking units. Notably, the participants highlighted 3 types of units. The units are “specialist unit” (PRO11), “central unit” (PRO15) and “designated cyberstalking unit” (PO17). Hence, PRO2 expressed frustration that the lack of a clear point of contact leads to police officers going on “a wild goose chase”;

PRO2: “There are no clear points of contact for international and domestic cases. This could result in police officers going on a wild goose chase while victims are still being harassed by cyberstalkers. This problem is tiresome for prosecutors who are keen to prosecute but cannot prosecute because of delays in the investigation process”.

247
Like PO2 and PRO11, PRO27 expressed frustration at the lack of a designated unit to make it easier for prosecutors to liaise with specialist police officers;

PRO27: “A challenge that comes to mind is that there is no designated cyberstalking investigating unit in the UK to centralize the investigation process and to make it easier for prosecutors to liaise with specialist police officers. Such a specialist unit will make it much easier for prosecutors to liaise with specialist officers”.

PRO23 in his extract below, echoed the frustrations of the participants and also, highlighted the additional problem of lack of finance;

PRO23: “There is the resources side of the problem. By that I mean a lack of resources both financially and manpower wise. Then there is also the issue of what units that are out there to use. Are there any specialist units that can help? If so where are they? Who do we contact?”

Like PRO23, PRO28 expressed the view that a specialist unit was required. Hence, he remarked from a financial perspective, “there is an option of setting up a specialist unit but it costs money to set up and run it”.

Moreover, PO20 shared the perception that there was no centralized database for gathering and accessing local intelligence on cyberstalkers at the time of the study. PO20 explained that at the time of the study, police officers were unable to access the database of another police force. PO20’s extract reveals that police officers are frustrated when such an investigative issue prolongs the ordeal of victims;

PO20: “To start with, the police face difficulties with accessing local intelligence because most foreign law enforcement agencies are not willing to share intelligence. This can hamper the investigation of such cases. Would you believe that in this country for example, police officers like myself cannot search the database of another police force without going through a lot of red tape? This can slow down the investigation process? For example, I am investigating a Cambridge job and cannot even access the local police database of the
Cambridge police force and this slowing my investigation of a particular offence. In the middle of this is a victim. Situations like these are so frustrating for the police officers especially when victims are involved. How do you then tell the victim that a different police force is holding up the investigation of a crime thereby prolonging the dilemma of the victim at the hands of the cyberstalker? It is ridiculous and this is an aspect of the investigation that needs to be addressed. Do you see what I mean? Because the offence is not taken seriously”.

Like PO20, PRO1 expressed frustration at the lack of a centralized cyberstalking database in the UK;

PRO11: “There are no specialist cyberstalking units in the UK. What this means is that if a cyberstalker is residing in a different part of the UK and the victim is in a different part of the UK, it might not be a straightforward process for the different police officers to work together and share intelligence promptly”.

Although the participants referred to different types of units, they all shared the view that the purpose of the units would be to “equip the units with specialist officers who will “offer guidance to police officers” (PO9), “provide assistance to colleagues who need them” (PRO23), and “enable UK police officers to obtain assistance from the right officials from the start to the end of a cyberstalking case” (PO25).

Similarly, PO21 emphasised how the units will be beneficial to police officers. Notably, PO21 said “the units will make it easier for me to make contact with the right people from the beginning of the investigation to the conclusion”.

Int: What problems are you aware of that hinder the prosecution of cyberstalkers?

PO21: “A designated unit should be created”.

Sub Question: “In your opinion, how would such a unit assist law enforcement officials?”
PO21: “It will ensure that I get the right experiences when investigating the case because I will be liaising with the experienced and appropriate law enforcement officials. Also, it will make it easier for me to make contact with the right people from the beginning of the investigation to the conclusion”.

It is important to note that in contrast to the above view on lack of resources, PO17 was keen to point out in his extract below, the existence of the National Cybercrime Reporting Centre;

PO17: “At the moment the crime is poorly reported. What we have done is create a National Cyber Crime reporting centre. Intelligence is disseminated from this centre to the City of London to the police”.

In conclusion the participants shared the perception that issues pertaining to lack of resources frustrate them in the investigation and prosecution of cyberstalkers. Given that cyberstalking is committed in the virtual realm, some of the participants attributed the issue of lack of resources to the cyberstalking not being perceived as a serious offence in comparison to other major offences which are committed in the physical realm. Therefore, PO22 in explaining why lack of resources is an investigative problem, remarked that “the offence is not taken seriously”.

4.3.5 Theme 5: Risk assessment challenges

‘Risk assessment’ was the fifth main theme identified in the study. Importantly, all of the police officers and 94% of the prosecutors shared the perception that five perceived risk assessment challenges frustrate them during investigation and prosecution processes because the challenges jeopardize the safety of victims. The perceived risk assessment challenges are; i) police officers not being able to risk assess anonymous cyberstalkers, ii) cyberstalkers breaching restraining orders, iii)
lack of resources, iv) lack of knowledge, v) victims in domestic violence cases rekindling relationships with cyberstalkers and vi) victims refusing to implement recommended risk assessment safety measures.

The police officers and prosecutors identified 13 and 10 perceived risk assessment issues respectively which frustrate them in the investigation and prosecution of cyberstalkers. The perceived risk assessment issues are presented in Table 4.12.
Table 4.12: Perceptions of police officers and prosecutors on risk assessment

<table>
<thead>
<tr>
<th>Perceptions of prosecutors on risk assessment</th>
<th>Number of police officers</th>
<th>Percentage of sample</th>
<th>Number of prosecutors</th>
<th>Percentage of prosecutors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks posed by anonymous cyberstalkers cannot be assessed</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Anonymous cyberstalkers cannot be managed</td>
<td>3</td>
<td>12</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Anonymous cyberstalkers cannot be identified</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>The actions of anonymous cyberstalkers are unpredictable</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unveiling the identities of anonymous cyberstalkers</td>
<td>2</td>
<td>8</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>Impossible to eliminate risks to victims absolutely</td>
<td>2</td>
<td>8</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Some victims are unaware of risks</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Challenging to risk manage victims in general</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Managing risks in domestic violence cases specifically</td>
<td>4</td>
<td>16</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>Victims refusing to implement recommended risk assessment safety measures</td>
<td>2</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Table 4.12: Perceptions of police officers and prosecutors on risk assessment

<table>
<thead>
<tr>
<th>Perceptions of prosecutors on risk assessment</th>
<th>Number of police officers</th>
<th>Percentage of sample</th>
<th>Number of prosecutors</th>
<th>Percentage of prosecutors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Educating victims on risk assessment safety measures</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Breach of restraining Orders</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Cyberstalking via proxy</td>
<td>2</td>
<td>8</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Victims refusing to be risk assessed</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>25</td>
<td>100</td>
<td>27</td>
<td>92</td>
</tr>
</tbody>
</table>

The participants expressed their frustration at their inability to investigate and prosecute anonymous cyberstalkers whose identities are unknown. Particularly, the Participants stressed that they cannot assess the risks to victims that are posed by anonymous cyberstalkers. Hence, PO6 expressed frustration that victimisation cannot be stopped if the perpetrator is anonymous. Notably, PO6 in the last sentence of his extract, said that it is vital to establish the identity of an anonymous cyberstalker to enable police officers to risk assess victims;

PRO6: “The main problem is the anonymity of cyberstalkers. Also, it doesn’t necessarily mean an alleged cyberstalker sent the messages as his computer could be hacked. The worrying thing is that most people won’t know how to tackle a cyberstalker if the identity of the cyberstalker is anonymous. I feel that
it is crucial to verify the identity of a cyberstalker to enable us to risk assess victims”.

Sub Question: In your opinion, why is the identity of cyberstalkers crucial for risk assessment purposes?

PRO6: “It is crucial because the police cannot risk assess victims if the identities of cyberstalkers are not known. They are therefore tasked with unveiling the identities of cyberstalkers which is difficult”

Like PO6, PRO22 explained that it is difficult for police officers to assess the dangers posed by anonymous cyberstalkers to victims.

Int: What difficulties in your opinion do the police face in the prosecution of cyberstalkers?

PRO22: “Police officers cannot access the risks posed by cyberstalkers who are anonymous. Risk assessments work when the identities of the offenders who pose threats or a danger to victims are known. It is difficult to establish the threat posed by anonymous cyberstalkers because the police officers do not know who they are”.

Given that the internet affords users the opportunity to create fake online identities and to harass victims at random, the participants stressed that another issue which frustrates them is that anonymous cyberstalkers are unpredictable which makes it difficult for police officers to monitor their actions. Hence PRO12 discussed how the unpredictable activities of cyberstalkers who use multiple identities impede the risk assessment of victims.

Int: What difficulties do the police face in the prosecution of cyberstalkers?

PRO12: “I will say evidential difficulties in terms of not being able to prosecute anonymous cyberstalkers. It is also a difficulty for police officers if they cannot carry out risk assessments because a cyberstalker has used various fake online
identities. The challenge for police officers is to establish the correct identities of cyberstalkers in order to risk assess victims. The two main challenges that police officers will have to overcome are that some cyberstalkers victimise via third parties and also use publicly accessible computers to send obscene and threatening messages to victims from numerous fake internet accounts”.

Similarly, PO13 expressed frustration that the unpredictable actions of anonymous cyberstalkers leaves victims on “tenterhooks”;

PO13: “The difficulty that is a major investigative headache is anonymous cyberstalkers. Would you believe that in some cases, the risks posed by anonymous cyberstalkers cannot be subsequently monitored if initially identified? Because anonymous cyberstalkers are unpredictable, victims are left on tenterhooks”.

Like PRO12 and PO13, PO21 shared the perception that it is challenging to risk assess anonymous cyberstalkers;

PO21: “I would say unveiling the identities of anonymous cyberstalkers. This issue has arisen because cyberstalking occurs in the cyber realm and does not require perpetrators to have physical contact with victims. This is obviously a dilemma for police officers because they cannot conduct risk assessments if cyberstalkers cannot be identified”.

Similarly, PO25 echoed the views of PRO12 and PO21. Notably, PO25 indicated that he could not conduct a risk assessment in a case because the cyberstalker was anonymous;

PO25: “Anonymous cyberstalkers are a real stumbling block for us simply because it stops us from risk assessing both the cyberstalkers and victims. The worry is that we cannot risk assess the danger that victims are in if we do not know who the cyberstalkers are. I once investigated a case involving an anonymous cyberstalker but could not conduct a risk assessment because the cyberstalker was anonymous”.

255
While discussing the unpredictable actions of cyberstalkers as an impediment to the risk assessment of victims, the participants shared the frustration that victims in some cases, may be unaware of the risks that they face from cyberstalkers. PO14 explained that in such cases, victims become aware that they are being cyberstalked only after their dilemma has been brought to their attention by a third party;

PO14: “A concern is that in some cases, victims may be totally unaware that they are in danger and are being cyberstalked until a third party brings it to their attention. This situation arises in cases involving cyberstalkers who create fake email and internet accounts in the names of unsuspecting victims and then disseminate offensive messages in the names of victims after hacking into their internet accounts. It is a concern because we cannot risk assess victims who are not aware that they are being victimised”.

Similarly, PRO22 expressed frustration at cyberstalking victims for example who “refuse to make formal complaints to the police despite their ordeal”. PRO22 explained that the issue of underreporting prevents the risk assessment of victims. However, unlike PO14, PRO22 referred to victims who are aware that they are being cyberstalked and have nevertheless, chosen not to report such incidents to the police.

Likewise, POI expressed frustration at some victims not being aware of the potential risks faced by victims is an issue. Therefore, PO1 reiterated in the last sentence of his extract that the real problem is trying to manage the risk that the victim faces at the hands of cyberstalkers;

PO1: “In summary, a combination of factors will affect the effective investigation of cyberstalkers such as barriers to understanding the seriousness of the offence, the lack of understanding of potential risks faced by victims, failure of victims to pursue a complaint, evidential problems and a poor cultural attitude by the law enforcement officers. In theory, it should be easy to track down the
cyberstalker once a complaint is made given that the crucial evidence are on the computer. The reality, is trying to manage the risk that the victim faces”.

In common with, PO19, PRO3, PRO17 and PRO23, PO10 explained that the continued victimisation of individuals by persistent cyberstalkers, frustrates police officers because sometimes, convicted cyberstalkers breach restraining orders and then commit further offences against victims. PRO10 in his extract, powerfully illustrated that some cyberstalkers are not deterred by restraining orders;

PO10: “Sometimes offenders continue to offend despite legal sanctions. For example, I reviewed a rape case which involved a cyberstalker who had been in a relationship with the victim. The cyberstalker raped the victim after breaching a restraining order and then hacked her email account and sent out obscene messages in the victim’s name. The police officer who investigated the case was frustrated by the case because the case demonstrates that restraining orders may not deter cyberstalkers in certain cases. The problem is that victims in such domestic violence cases will continue to be at risk from persistent offenders”.

While discussing the difficulties the police face in the prosecution of cyberstalkers, the participants expressed frustration at victims who are aware of imminent risks at the hands of cyberstalkers but refuse to implement recommended safety measures after being risk assessed. PO7’s extract demonstrates the frustration felt by police officers when victims refuse to implement recommended risk assessment safety measures;

PO7: “In addition to investigative difficulties, an issue which I feel needs to be highlighted is that sometimes, victims refuse to implement recommended risk assessment safety measures after being risk assessed. This is a nightmare for police officers because such decisions, jeopardize the efforts of police officers to manage the risk to victims.

Like PO7, PO21 discussed the reluctance of some victims to implement recommended risk assessment safety measures. Although PO21 acknowledged the reasons given
by victims at the end of his extract, he stated that personal safety should take priority over pride;

PO21: “It is frustrating for police officers when victims do not implement risk assessment safety measures. I say this because, some of the victims that I risk assessed refused to change or remove their personal details from the internet because of business implications and because, they did not want to give the cyberstalkers the satisfaction that they were controlling their lives. In the grand scheme of things, personal safety comes first before pride”.

Given the risk assessment difficulties highlighted by the participants, many of the participants shared the perception that managing the risks to victims in domestic violence cases specifically is frustrating. Particularly, PRO20 highlighted the issue of victims having intermittent relationships with cyberstalkers which makes it difficult for police officers to guarantee the safety of victims. PRO20’s extract, powerfully illustrates the frustration felt by police officers, as demonstrated in the end of the extract, wherein PRO20 questioned how police officers are expected to risk assess victims who are refusing to cooperate;

PRO20: “Police officers sometimes, encounter problems in risk assessing domestic violence victims if the victims still want to maintain relationships with the cyberstalkers especially if she has a child with the cyberstalker. This situation may result in the victim refusing to be risk assessed. This can be frustrating for us especially when we are aware of the risks and can foresee the danger that victims are in”.

When discussing the factors which hinder police officers from risk assessing victims in domestic violence cases, the participants also expressed the view that sometimes, victims withhold information on the gravity of the cyberstalking incidents that they have been subjected to. The participants revealed that this lack of disclosure prevents police
officers from fully establishing the risks or potential risks that victims face. PRO14’s extract, powerfully illustrates the frustration felt by police officers;

PRO14: “Victims withholding crucial evidence. When victims decide to rekindle relationships with former partners who are under investigation for cyberstalking and domestic violence offences, such decisions place victims at risk from the cyberstalkers because they can be unpredictable. It is equally infuriating for police officers because it wastes the time of police officers who are trying to keep victims safe from potentially dangerous cyberstalkers”.

The participants discussed how evidential difficulties, can hinder the risk assessment of victims. Hence, PRO9 confirmed the views of the participants especially in relation to victims in domestic violence cases withholding evidence;

PRO9: “There is also the issue of risk assessing victims in domestic violence cases who appear to still want a relationship with the cyberstalker. Obviously in domestic violence cases, risk assessments will be conducted to protect the victim and police officers will be required to manage the identified risks. But how can the risks be managed in domestic violence cases for example where the victim is still in contact with the cyberstalker and subsequently decides not to support a prosecution? In such cases, the cyberstalker’s activities could be a means of controlling a victim who has been in an abusive relationship for a while. Another issue is that if the victim in a domestic violence case does not reveal the true scale of a cyberstalker’s harassment, the police may be unable to accurately assess the severity of the situation”.

The participants also, shared the view that it is challenging for police officers to conduct risk assessments when cyberstalkers victimise via proxy. Hence, PO22 stated that “cyberstalking via proxy is an impediment to the risk assessment of victims especially if it involves anonymous cyberstalkers using unsuspecting third parties to target victims”.

259
While discussing the evidential challenges in investigating domestic violence cases, the police officers expressed frustration at not being able to conduct investigations quickly to avoid fatalities. Consequently, PO5 described the situation as a “vicious cycle” and asserted in the last statement of his extract that “there are no absolute guarantees with the management of risks”;

PO5: “If the cyberstalker is in the UK, we have to speed up the investigation and do things much quicker to avoid any fatality and vice versa. The difficulty is how can we as police officers be sure that an anonymous cyberstalker is not abroad? Which brings us back to having to rely on the evidence. Most of the time, there is no evidence because the cyberstalker is usually anonymous and as such, we rely on the victim and we advise them to keep records of any emails or computer messages from the cyberstalkers. Do you see the predicament we face? It is a vicious cycle to investigate. To investigate properly, we need the evidence and at the moment, we are struggling to get the evidence. There are no absolute guarantees with the management of risks to victims”.

Remarkably, PO6 acknowledged that there is a possibility that a police officer may make an error in risk assessing victims because he will be required to establish the realistic risk to a victim based on his personal judgement. It is important to note that no other participant shared this view;

PO6: “The initial difficulty is the risk management because an investigating police officer will need to establish the realistic risk to the victim. Because it is subjective and based on an individual police officer’s judgement, there is a possibility that a police officer might get it wrong. If a victim has reported an incident after 6 months, it is less likely to be serious compared to if a victim has reported an incident immediately after it happened”.

While discussing the difficulties that the police face in the risk assessment of victims, PO17 highlighted that if required, the police take special measures to protect victims. Hence PO17 in his extract, discussed the measures that were implemented to guarantee the safety of a victim in a domestic violence case. However, PO17 did not confirm if this was common practice;
PO17: “Risk assessing victims. This is not always possible if the cyberstalkers cannot be identified”.

Int: Did you take any measures to protect victims?

PO17 “Yes. In a case that I investigated, the victim’s address was put under a special scheme which meant that any phone call from her address was treated as urgent and received a quicker response. She was also given advice on what to do and the safety measures to take”.

While discussing the risk assessment of cyberstalkers whose identities are known, some police officers shared the frustration that it was impossible to eliminate the risks to victims even if the identity of a cyberstalker is known. The participants expressed the view that the safety of victims cannot be absolutely guaranteed because sometimes, cyberstalkers breach restraining orders which prohibit offenders from contacting victims. Echoing this view PO19 discussed the risk assessment of cyberstalking victims in domestic violence cases;

PO19: “The issue that we face in terms of protecting victims is that police officers cannot always predict if former partners will breach restraining orders or murder their partners because absolute guarantees cannot be given in the management of risks. It is very frustrating when cyberstalkers breach restraining orders because, they jeopardize all the risk assessment safety measures that have been put in place to protect victims”.

It is of note that, PRO5 reiterated the view of PRO19 by highlighting the case of Claire Bernal who was murdered by her former boyfriend after being stalked face to face and cyberstalked via phone;

PRO5: “The Protection from Harassment Act has been around since 1999 so more officers are aware of the legislation. Also, the case of Claire Bernal who
was cyberstalked by her ex-partner and then murdered in the Harvey Nichols shop, puts the case in the public agenda. The defendant later killed the victim while on bail even though a restraining order was in place. The case did a lot for the government to make them take the offence seriously."

In conclusion, the majority of the participants expressed their frustration at several factors which hinder the police officers from risk assessing and managing the risk to victims. The factors include anonymous cyberstalkers, victims refusing to implement recommended risk assessment safety measures, breach of restraining orders, victims in domestic violence cases rekindling relationships with cyberstalkers and underreporting.

4.3.6 Theme 6: Evidential challenges

‘Evidential difficulties’ was the sixth main theme that emerged from the interview data. Crucially, all of the police officers and 91% of the prosecutors shared the perception that various perceived evidential difficulties frustrate them during the investigation and prosecution of cyberstalkers. The perceived evidential difficulties are delays by police officers in providing outstanding evidence, inability of prosecutors to make charging decisions due to insufficient evidence, reluctance of domestic violence victims to support the prosecution of cyberstalkers, establishing offences under the PHA, the inability of police officers to trace anonymous cyberstalkers to unregistered cards and the inability of police officers to unveil the identities of anonymous cyberstalkers.

The police officers and prosecutors identified 11 perceived evidential difficulties which frustrate them in the investigation and prosecution of cyberstalkers. The perceived issues are presented in Table 4.13.
Table 4.13: Perceptions of police officers and prosecutors on evidential challenges

<table>
<thead>
<tr>
<th>Perceptions of participants on evidential difficulties</th>
<th>Number of police officers</th>
<th>Percentage of sample</th>
<th>Number of prosecutors</th>
<th>Percentage of prosecutors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victims not keeping evidential records</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Police officers not providing further evidence once suspects have been charged</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>Prosecutors having to repeatedly chase police officers for evidence</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Not obtaining CPS charging decisions due to lack of evidence</td>
<td>3</td>
<td>12</td>
<td>5</td>
<td>17</td>
</tr>
<tr>
<td>Establishing a course of conduct under section 7 of the PHA</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Cases having to be discontinued due to a lack of evidence</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Obtaining evidence from victims in domestic violence cases</td>
<td>6</td>
<td>24</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>Insufficient evidence to prosecute</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>10</td>
</tr>
</tbody>
</table>
Table 4.13: Perceptions of police officers and prosecutors on evidential challenges

<table>
<thead>
<tr>
<th>Perceptions of participants on evidential difficulties</th>
<th>Number of police officers</th>
<th>Percentage of sample</th>
<th>Number of prosecutors</th>
<th>Percentage of prosecutors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domestic violence victims not reporting cases</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Proving a case under s4A of the PHA</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Anonymous cyberstalkers are one step ahead of police officers</td>
<td>2</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Evidence in the cloud</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unregistered SIM cards</td>
<td>2</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Registered SIM cards</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Using lost or stolen phones</td>
<td>2</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Impact of disclosure on victims</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Prosecuting mentally ill Cyberstalkers</td>
<td>3</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Police delays in providing evidence</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>25</td>
<td>100</td>
<td>28</td>
<td>91</td>
</tr>
</tbody>
</table>
While discussing how lack of evidence can hinder prosecutors from making charging decisions, the prosecutors expressed frustration at not being able to obtain evidence from the cyberstalking victims in domestic violence cases.

PO10’s extract illustrated the participant’s frustrations at victims withholding crucial evidence from the police. The tone of PO10’s extract demonstrates this in relation to the perceived problem of victims withholding evidence from the police;

PO10: “Obtaining evidence from the victim may be challenging in domestic violence cases which involve victims who no longer wish to support the prosecution of offenders. This can be infuriating if it results in charges being withdrawn”.

Similarly, while discussing evidential difficulties which impede prosecutors from charging offenders, PO14 expressed frustration at the inability of some police officers to provide all the evidence that the prosecutors require to charge offenders within CPS deadlines. However, PO14 acknowledged that the delay in providing evidence after suspects have been charged was due to the fact that police officers have to prioritise their work and are under pressure which may lead to other cases that are perceived to be more serious, being investigated first;

PO14: “The CPS always require more evidence after suspects have been charged. The problem is that we prioritise our work and may not provide the evidence required when the prosecutors want them. We are under a lot of pressure to provide additional evidence in several cases”.

Likewise, PO19 echoed the views of PO10 and PO14. However, PO19 suggested that the delay by police officers in providing outstanding evidence is linked to the high CPS evidential threshold;
PO19: “A major problem is meeting the high CPS evidential threshold because, the prosecutors may request additional evidence which make take a while for us to obtain. I think that the evidential threshold is very high which is why we struggle to meet the threshold in some cases”.

Similarly, the participants shared the perception that evidential difficulties can hinder them from proving cases due to this high evidential threshold PR020 highlights this in the following extract;

PRO20: “Proving a case is dependent on whether prosecutors can satisfy the evidential and the public interest tests. The evidential threshold is very high. The threshold can only be met if police officers provide the necessary evidence. Obtaining the evidence however, can be challenging”.

While discussing the difficulties police face in the prosecution of cyberstalkers, the participants shared the frustration that prosecutors find themselves having to repeatedly request outstanding evidence from police officers. Therefore, PRO7 explained that it is frustrating for prosecutors when they have to repeatedly chase police officers for outstanding evidence because it prevents prosecutors in some cases from making charging decisions. However, at the end of their extract, PR07 acknowledges that police officers are overworked;

PRO7: “The length of time that it takes for police officers to provide the required evidence. This issue is frustrating for us because it results in prosecutors having to repeatedly chase police officers for outstanding evidence. The police always say that they are investigating several cases at the same time. Some do not realise that we as prosecutors cannot prepare robust cases against suspects without the required evidence. Most of the officers in my cases tell me that they are overworked”
Like PRO7, PRO22 stated that prosecutors are unable to progress cases due to lack of evidence from the police. Particularly, PRO22 said that CPS charging decisions may not be provided due to lack of evidence from the police. Hence, PRO22’s extract highlighted his frustration that the ordeal of victims at the hands of cyberstalkers, will be prolonged due to the delay by police officers in providing outstanding evidence. Importantly, at the end of the extract, PRO22 linked the problem of lack of evidence to the misguided perception that cyberstalking is not a serious offence;

PRO22: “Due to lack of evidence, a charging decision may not be promptly obtained from the CPS. Prosecutors can only make prompt charging decisions once all the required evidence is provided by the police. Prosecutors can only decide if there is sufficient evidence to charge a person when the police provide the evidence that they have against an accused. In my view, an evidential challenge is not obtaining prompt charging decisions due to lack of evidence. The problem has arisen because not everyone considers cyberstalking a grave offence”.

Similarly, some of the of the participants linked the highlighted evidential difficulties to the perceived problem of police officers prioritising cases perceived to more serious over cyberstalking. Hence PO16 explained that cyberstalking is an offence which is committed in the cyber realm and will be therefore be “at the bottom of the pile” because it is perceived to be a “self-inflicted” offence by some people;

PO16: “Police officers dealing with more serious cases may be reluctant to prioritise a cyberstalking case because it merely involves harassment conducted in cyber space. I think that cases involving online harassment will be at the bottom of the pile because cyberstalking is a new offence which is perceived by some as self-inflicted because it is not mandatory for people to be part of the social media world given the dangers that are associated with being part of the online world. As a result, the offence may not be taken seriously. Also, if there is no obvious danger to the life of the victim, trying to establish whether a cyberstalker poses a real or current risk may delay the investigation of such cases”.
PRO30 echoed the frustrations of PRO7, PRO22 and PO16 that some police officers do not realise that they are still required to submit additional evidence after a cyberstalker has been charged. At the end of his extract, he stressed that prosecutors are tasked with contacting police officers repeatedly for outstanding evidence to ensure that cases are progressed;

PO1: “Obtaining the required evidence from the police promptly. Police officers do not realize that they are still required to submit additional evidence after a cyberstalker has been charged. If the evidence is provided promptly, prosecutors are able to charge cyberstalkers with appropriate offences. The problem is that prosecutors like end up contacting the police repeatedly for previously requested evidence after charge”.

While discussing the cyberstalking issues that need to be addressed, the participants shared the perception that it will be difficult to obtain advice from prosecutors to charge a cyberstalker under s4 of the PHA if the cyberstalker is anonymous. PRO22’s extract highlighted his frustration at anonymous cyberstalkers evading justice after committing offences under s4 of the PHA. However, at the end of the extract, PRO22 reveals that sometimes, cyberstalking is linked to other criminal conducts and consequently, it may be difficult to promptly build a case against an accused because the other charges may take prosecutors a long time to review;

PRO22: The issue is with the evidential gathering process to proof that anonymous cyberstalkers have committed offence of causing fear of violence has been committed under s4 of the PHA. This in my opinion is an annoying issue which makes the jobs of police officers and prosecutors so much more difficult because we cannot prosecute without the relevant evidence. We cannot prove that there is sufficient evidence to realistically prosecute a cyberstalker if the cyberstalker is anonymous. This may lead to them evading justice. Another problem is that sometimes, cyberstalking is associated with other criminal conducts such as threats to kill, criminal damage and so on which are linked to
stalkling and harassment but yet, it may be difficult to build a case against a suspect because of the other charges may take prosecutors ages to sift through”.

Similarly, the participants expressed the view that because cyberstalking is not perceived to be as serious as face to face stalking, it is difficult to show that a fear of violence has been committed in certain cases under s4 of the PHA. PRO19 in his extract, powerfully illustrated that some cyberstalkers are not deterred by restraining orders;

PRO10: “I once reviewed a cyberstalking case. Due to the fact that the harassment was not deemed to be an immediate threat to the victim’s life, the actions of the stalker fell short of creating the fear of violence. We could not prove that the cyberstalker created a fear of violence. Not being able to satisfy such legal requirements can unfortunately mean that cases cannot be proved. This obstacle can constitute a stumbling block for prosecutors”.

Int: In your opinion what other legal requirements can determine if cases be prosecuted?

PRO10: “There are several areas of legal difficulties that can be infuriating such as police officers not being able to obtain sufficient strong evidence to connect suspects to cases. This Evidential Test needs to be satisfied under the code for crown prosecutors. Without the evidence, we cannot build cases. Then there is the legal issues of having to prove that a cyberstalker’s actions towards a victim created fear of violence to make out the offence. The other legal issue that I can think of is the fact that a cyberstalker can claim that a third party hacked into his computer and disseminated offences messages to the victim in his name. This area of legal difficulty will require us to rely on expert digital forensic expert evidence to connect a cyberstalker to an offence. So specialist knowledge will be required”.

Given that prosecutors cannot prove that there is a realistic prospect of convicting offenders without sufficient evidence from the police, some prosecutors expressed frustration that cases may be discontinued due to lack of evidence. The participants expressed the view that the inability of police officers to provide outstanding evidence
within stipulated court deadlines can become exasperating for prosecutors because it can lead to the prosecution missing various deadlines to comply with court directions. PRO22 in his extract, powerfully illustrated the frustration of the prosecutors who perceive lack of evidence as a factor which leads to cases being discontinued;

PRO22: “Police officers not promptly provide outstanding evidence from victims or not providing the evidence required to build cases against cyberstalkers. This issue is never ending for prosecutors because they constantly have to chase police officers and their supervisors for outstanding evidence. This is more frustrating because the lack of evidence can lead to offenders not being charged and cases being discontinued”.

Likewise, the prosecutors shared their frustration at not being able to build strong cases against offenders in some domestic violence cases due to insufficient evidence. Hence, PRO26 emphasised that an issue which frustrates them is that it may be difficult to meet the CPS evidential threshold. However, at the end of the extract, PRO26 expressed the concern that the evidential problem will stop victims especially in domestic violence cases from reporting incidents;

PRO26: “We are constantly faced with the problem of police officers providing insufficient evidence which means that in some cases prosecutor cannot satisfy the Evidential Test that there is sufficient evidence to provide a realistic prospect of conviction against a suspect on each charge. The bigger worry for me is that victims will lose faith in the criminal justice system if they report cases of cyberstalking and are told by the police that there is insufficient evidence to take the cyberstalkers to court. This may stop victims from reporting cases. It is very concerning because in some domestic violence cases, cyberstalking can lead to fatalities”.

Similarly, PRO25 expressed frustration at the inability of police officers to investigate and prosecute anonymous cyberstalkers;
PRO25: “There is the problem of identifying the cyberstalker. How can we get him to trial if we cannot find him? If we do not know his identity? Assuming that you eventually get a cyberstalker to court, how do you prove that the cyberstalker was the originator of the message? You will need to provide expert report to say that the message came from his computer and confirming that the computer was not hacked into. You will have to establish that the computer was secure. It will have to be shown that the cyberstalker had physical access to the computer. In relation to the contents of the messages, it has to be determined whether the contents of the messages pass the test of harassment or malicious communications. In relation to the internet service providers, the issue of proportionality will need to be addressed. We struggle to get them to cooperate with serious offences let alone cyberstalking offences”.

Like PRO25, PO21 expressed frustration that it will be challenging for police officers to prosecute cyberstalkers due to evidential difficulties. Worryingly, in the last sentence of his extract, PO21 concluded that “we can overcome the technical difficulties but we cannot overcome the evidential difficulties”;

PO21: “Because we as police officers may track online malicious activities to a cyberstalker but will then face the difficulty of proving that the cyberstalker sent the offensive messages for example if he claims that he was living in a shared accommodation and as such, anyone could have used the computer to send the messages. The problem we then face has to prove that such an alleged cyberstalker used the computer. How for instance do you establish that an alleged cyberstalker sent the offensive online messages when he claims that a third party hacked into his computer? How does a police officer prove the time that it was sent, the location, the identity of the sender and the identities of the various people who could have potentially accessed the computer or had access to the computer? Police officers therefore face technical difficulties in trying to investigate the conduct by the very nature of the definition of the conduct”.

While discussing the issues which define cyberstalking, PRO24 talked about evidential challenges that prosecutors and police officers encounter when prosecuting offenders in domestic violence cases. Particularly, PRO9 highlighted the issue of victims subsequently wishing to maintain relationships with cyberstalkers after making formal
complaints. PRO9 explained that this issue is particularly frustrating in child custody cases especially because it results in victims withholding evidence from the police;

PRO24: “An issue is how cyberstalkers in domestic violence cases define course of conduct under the PHA. I prosecuted a case involving a cyberstalker who argued that his actions were reasonable because still wanted to maintain a relationship with the victim”.

Int: In your opinion why is it challenging to investigate cyberstalkers in domestic violence cases?

PO24: “The main reason is that the victim may still want a relationship with the cyberstalker especially if she a child with him and as such, may not reveal all the threatening messages that she has been receiving from him. The problem is that prosecutors require the electronic evidence to build strong cases against cyberstalkers and to show that there is a realistic prospect of convicting them. The legal issue which frustrates us is that we cannot prosecute cyberstalkers without sufficient evidence. We are led by the victims. If the victim says that she consented to the conduct, can we prove that an offence has been committed? The victim has to spell out the nature and effect of the conduct”.

The participants also, expressed frustration at cyberstalkers who victimise via phones and then try to evade justice by claiming that they did not harass the victims because their phones were either lost or stolen. Notably, PO23 revealed that he had lost a lot of cases because the police could not prove that suspects who claimed that their phones were lost or stolen, sent telephone messages or internet messages to specific victims;

PO23: “I used to work in the Domestic Violence Unit and investigated harassment cases some of which related to cyberstalking coming to think of it…… For example I had cases where the victim was receiving text messages, annoying telephone messages persistently from the suspects. Sometimes the suspects will call the victims at odd times of the night and then hang up the telephone. I lost a lot of the cases because we could not prove that the suspect sent the telephone messages or internet messages because although the
telephones were registered to them they often claimed that their telephone was stolen or lost and that they did not send the messages. So you had victims who were still suffering and receiving telephone calls at the middle of the night”.

Similarly, the participants expressed their frustration at how difficult it is to gather evidence against cyberstalkers who use ‘pay as you go’ phones with unregistered SIM cards to harass victims;

PO14: “I have investigated cases involving cyberstalkers who use emails, letters, Twitter, Facebook to harass victims and most of the time the suspect do not use correctly registered phone or ISP details. I think they give false information to the ISPs. I am dealing with one which has been going on for years. This guy has been phoning and texting his victim using unregistered SIM cards and phones. I have been doing several checks. He has used at least 30 different SIM cards and our records show that he has used different systems to harass the victim. Now the victim is on anti-depressants and her kids have a phobia of answering the telephone, this situation is frustrating not only for me, but for the poor victim”.

Int: In your opinion, why is the issue frustrating?

PO14: “Because, most of the times as I explained, the cyberstalker uses false details to obtain to obtain his phones or to register with ISPs or sometimes buys phones with unregistered SIM cards. It then requires a lot of police time resources and procedure to track down the cyberstalker. In many of my cases, the cyberstalkers registered false details with Virgin Media, The current case that I am investigating has led me to Greenfield, Derby and all across the country”

Like PO14, PO16 expressed frustration that some anonymous cyberstalkers who offend via the use of unregistered mobile phones evade justice because they cannot be traced by police officers. PO16 expressed additional frustration that the investigation of such futile cases, leads to the wastage of limited police resources;
PO16: “One of the major problems is that the cyberstalkers use unregistered phones it is difficult to track them down as a result, a lot of them cannot be traced. In addition, it is very time consuming to investigate the case and leads to the wastage of limited police resources in terms of manpower, time and finance...”

Sub Question: In your opinion, why is it difficult to trace such suspects?

PO16: “At the moment there is no requirement or legislation compelling customers to register their correct details once a phone is purchased or an internet account is opened. The anomaly makes it easier for the cyberstalkers to commit the crimes without arguably being traced”.

Like PO23, when discussing cyberstalkers who stalk victims using mobile phones to send obscene electronic text messages, P029 expressed frustration that in some cases, it was difficult for police officers to connect cyberstalkers who have registered telephones to offences which could result in cases being lost;

PO29: “There is a massive problem where you have a victim that shows you their mobile phone with a message that they received but we do not know where the message came from. The suspect might say that he did not send the message and that someone else stole his phone which was lost or that someone else used his phone without his knowledge. How can we prove that an offence has been committed in such a case even though the phone is registered to the suspect?”

The participants also expressed frustration that an anonymous cyberstalker cannot be prosecuted especially where he uses a phone that has been registered with fake personal details. Hence PRO7 said that “cyberstalkers are one step ahead of police officers;

PRO7: “The major one is that because it will be difficult to arrest, interview, and charge a cyberstalker if he is anonymous. This is where the issue with the evidential difficult arises. The other problem is that it will be difficult to prosecute a cyberstalker who uses a registered SIM card and several pay as you go
phones to target victims. This problem is kind of linked to the fact that cyberstalker can use false details to create fake accounts for cyberstalking. The problem as it stands today unfortunately puts cyberstalkers one step ahead of the police officers because cyberstalkers cannot be prosecuted unless they are identified and evidentially connected to offences, They know this too which is why some of them cover their tracks online.

While discussing the difficulties that police officers face in the prosecution of cyberstalkers, many of the participants also expressed frustration at the ISPs who do not promptly provide the required evidence which prolongs the ordeal of victims. Hence PRO26 highlighted in the last sentence of his extract, the issue of victims not having faith in the criminal justice system if offenders are not prosecuted due to evidential difficulties;

PRO26: “It is a pain to work with the network providers. In the midst of all this delay, there are victims who are still being harassed and whose harassment ordeal are ongoing. There is an issue with the evidence gathering process because it is difficult to obtain evidence from some of the ISPs. The danger is that it could result in victims losing faith in the criminal justice system”.

It is important to note that PO11 linked the reluctance of some ISPs to provide outstanding evidence to the perception that cyberstalking is not deemed by some to be a serious offence;

PO11: “ISPs should be made to promptly provide the information required on the same day to prevent the court from giving judges orders. The ISPs do not believe that cyberstalking is a serious offence which is why this problem exists”.

Like PO11, PO20 shared the perception that the ISPs are not very helpful in investigating cybercrime offences. In making this point, PO2O in his extract, referred to the online of 5 year old April Jones who was murdered by a paedophile after being
abducted. It is important to note that PO20 highlighted that cyberstalking can be linked to online grooming in certain cases;

PO20: “Police officers can’t get help from Facebook when required. This problem is becoming more and more relevant now and was apparent in the case of April Jones who was kidnapped, raped and murdered by a paedophile who assessed 400 websites depicting child sexual abuse online and pornography. This is a dangerous situation which can enable cyberstalkers who are paedophiles to target children”.

Likewise, PRO18 expressed frustration at the ISPs who were perceived to use data protection laws as an excuse for not releasing details of cyberstalkers. Hence, PO18 in his extract, highlighted that police officers sometimes, resort to seizing the computers of suspects to obtain the required evidence;

PO18: “The internet service provider should make it easier for the police to access information about cyberstalkers. Sometimes, they are not helpful and as a result, police officers are forced to seize the computers of victims in order to identify the cyberstalkers. This is unfair on victims. There should be a system similar to the medical consent forms to stop the internet service providers from using data protection laws as an excuse for not releasing the details of cyberstalkers”.

Int: In your opinion, why is it difficult to trace suspects?

PO18: “At the moment, there is no requirement for legislation compelling customers to register their correct details once a phone is purchased or an internet account is opened. The anomaly make it easier for cyberstalkers to commit the crimes with fake accounts without being traced”.

While discussing the difficulties that police officers face in the prosecution of cyberstalkers, the participants shared the perception that it is evidentially challenging
to obtain the subscribers details of alleged cyberstalkers from ISPs. Hence PO2 in his extract, echoed the views of the other participants;

PO2: “The ISPs, are usually hesitant to assist us which is an investigative obstacle. It is a challenge to obtain the IP addresses of subscribers suspected of alleged cyberstalking incidents. This issue creates an obstacle in the investigation process and thereby allows cyberstalkers to hide behind the veil of anonymity”.

While discussing people who do not take care of their phones thereby allowing such phones to be used by criminals to commit cyberstalking offences out of sheer frustration, PO3 expressed the view that such individuals should be penalized. PO3’s expressed frustration that he had lost some cases as result of this issue;

PO3: “Laws are required to penalise individuals who do not take adequate responsibility for their phones which are used to commit crimes. There should be legal sanctions because it makes it difficult for the police officers to investigate or prove such cyberstalking cases. I have lost a lot of cases on this point and it is frustrating”.

Similarly, PRO5 expressed the view that it is difficult to obtain evidence from the cloud which makes it challenging to trace victims;

PRO15: “The issue of offences occurring in the cloud makes it difficult to trace victims”.

While discussing alleged cyberstalkers who live in shared accommodations and share passwords with a third party, PO24 expressed the view that in such cases, it may be difficult to connect a suspect if the offenders claim that someone else sent
the messages to a victims. PO24 in line 2 of his extract, echoes the views of the participants;

Int: In your opinion, why is it evidentially difficult to build a case against a cyberstalker?

PO24: “Because we as police officers may track online malicious activities to a cyberstalker but will then face the difficulty of proving that the cyberstalker sent the offensive messages for example if he claims that he is living in shared accommodation and as such, anyone could have used the computer to send the messages because they all share the same password for the computer”.

Like PO24, PRO21 expressed frustration at police officers who cannot link anonymous cyberstalkers to IP addresses. PRO21’s extract echoes the views of the participants;

PRO21: “It is very difficult evidentially to build a case against a defendant. There is big reliance on IT or computer experts. It is a very difficult offence to prove. Plus harassment can occur by proxy. Also, people can send messages using another person’s account. For example when couples share passwords. Even if you obtain the IP addresses, it does not mean anything as people break into the IT addresses if they know how to. Also, there is an anonymous website which innocently implicates victims. The people who have set up the anonymous websites cannot be traced down as they may have 2,000 different sources. Paedophiles use these websites. Defendants are trying to be a step ahead. Evidentially, it is not easy to prove a case as you have to prove that the defendant used the IP addresses linked to offences”.

The participants also shared the view that the various evidential difficulties can result in cyberstalkers evading justice. Consequently, PRO9’s extract below reiterated the views of the other participants using the phrase “toxic mix of problems” to refer to the various evidential difficulties;

PR09: “Obtaining evidence is the primary issue. This can have an adverse impact on the investigation process and leading offenders not being prosecuted”.

278
Int: “In your opinion, how does the issue of evidential difficulty an adverse impact on the investigation process?

PR09: “Generally speaking it makes police officers become disillusioned because they are unable to do their job of investigating and prosecuting cyberstalking and also protecting victims due to the toxic mix of problems. It might lead to the time and effort that has been put into investigating cases going down the drain if cases cannot be proved due to a lack of evidence”.

Notably, PO23 explained that sometimes, “cases are lost on little things” because it is difficult to obtain all the evidence that the CPS requires to prosecute offenders. Remarkably, from a personal experience, PO23 also indicated that he felt that the existing law was not effective in protecting victims. PO23 in his extract, appeared to link his perception that the laws are “poor” to his believe that “cases are lost on little things”;

PO3: “My sister was cyber stalked by her ex-partner for a while and we found the law poor. Not very effective in protecting victims. It is very hard on the borough to get all the evidence that is required and to get what the CPS wants and then you end up losing the case on little things”.

Notably, the participants expressed frustration at the solicitors of mentally ill cyberstalkers who take a long time to provide medical evidence on a cyberstalker’s mental illness. Consequently, PRO15 said that it may be difficult to prosecute a cyberstalker who is mentally ill due to delays in trials caused by defence. In the last sentence of his extract, PO15 revealed that such delays leave victims feeling anxious;

PRO15: “An issue that is often overlooked is that it may be difficult to prosecute a cyberstalker who is mentally ill and requires treatment. In such cases his solicitors will inform the court that they will have the suspect assessed by a
psychiatrist to establish if he is fit to enter a plea. For prosecutors, it is frustrating when defence take a long time to provide the outstanding medical evidence which ends up delaying trials and making victims feeling anxious and desperate for trials to take place so that they can obtain closure”.

In conclusion, the above observations highlight the shared perceptions of the participants on how evidential difficulties hinder police officers and prosecutors form bringing cyberstalkers to justice. Table 4.13 indicates that the police officers and prosecutors, identified 11 areas of evidential difficulties.

4.3.7 Theme 7: Victim behaviour

‘Victim Behaviour’ was the seventh and final theme identified in the study. Crucially, all of the police officers and 95% of the prosecutors shared the perception that various, perceived, evidential difficulties frustrate them during the investigation and prosecution of cyberstalkers. The perceived issue of victim behaviour concerns victims not supporting prosecutions, refusing to testify, lack of full disclosure, cross communicating with cyberstalkers, withholding information and not reporting offences.

The prosecutors and police officers highlighted 11 and 13 (respectively) aspects of victim behaviour which frustrate them in the investigation and prosecution of cyberstalkers. These are presented in Table 4.14.
Table 4.14: Perceptions of police officers and prosecutors on victim behaviour

<table>
<thead>
<tr>
<th>Victim Behaviour</th>
<th>Number of police officers</th>
<th>Percentage of sample</th>
<th>Number of prosecutors</th>
<th>Percentage of prosecutor sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not supporting prosecutions</td>
<td>4</td>
<td>16</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>Refusing to testify</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>30</td>
</tr>
<tr>
<td>Refusing to go through the stress of trials</td>
<td>2</td>
<td>8</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Cross communicating with Cyberstalkers</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Lack of full disclosure</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Unwilling to spell out the effects and nature of incidents</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Lack of confidence in the police</td>
<td>3</td>
<td>12</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Withdrawal of allegations</td>
<td>4</td>
<td>16</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Table 4.14: Perceptions of police officers and prosecutors on victim behaviour

<table>
<thead>
<tr>
<th>Victim Behaviour</th>
<th>Number of police officers</th>
<th>Percentage of sample</th>
<th>Number of prosecutors</th>
<th>Percentage of prosecutor sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fear of repercussions</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Perception that cases will be dropped</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Breakdown of trust between the public and the police</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Not reporting offences</td>
<td>3</td>
<td>12</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Delays in reporting incidents</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Disclosing personal information on the internet</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Continuing relationships with Cyberstalkers</td>
<td>2</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Withholding information on the gravity offences</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Total</td>
<td>25</td>
<td>100</td>
<td>29</td>
<td>95</td>
</tr>
</tbody>
</table>
The participants expressed frustration at victims who do not report cyberstalking incidents to the police or delay before reporting such incidents. PO1 in his extract, demonstrates this viewpoint;

PO1: “From the victim’s perspective, the victim will experience an average of 100 episodes of stalking activities including cyberstalking before reporting the offence. The reluctance of victims reporting the conduct leads to victims evading justice and makes it difficult to assess the effectiveness of the legislation”.

Similarly, PRO14 expressed frustration at victims who refuse to support the prosecution of cyberstalkers. Particularly, those victims who subsequently make withdrawal statements;

PRO14: “Police officers face several difficulties in the prosecution of cyberstalkers. Unfortunately, the situation is not helped when victims refuse to support the prosecution of offenders. I have investigated cases involving victims who have subsequently withdrawn their statements prior to trials and after suspects have been charged.”

PRO17 also expressed frustration at victims who refuse to support the prosecution of offenders. In this extract, RPO17 reveals that this arises commonly in domestic violence cases and stated that it can leave prosecutors feeling frustrated if cases are consequently not progressed;

Int: Why do you feel that victims of cyberstalking are reluctant to support the prosecution of cyberstalkers?

PRO17: “In domestic violence cases, the reason is because some of the victims have a change of heart after reporting incidents because they do not want to see the father of their children being prosecuted. This really puts a spanner in the works for police officers and prosecutors who have put in so much time and
effort into such cases to bring offenders to justice. It is more exasperating for police officers and prosecutors if the CPS has no choice but to discontinue cases against cyberstalkers because victims have subsequently, withdrawn their allegations against the cyberstalkers. In such cases, the CPS cannot prosecute if there is therefore insufficient evidence to build a strong case against the offenders”.

Likewise, the participants expressed frustration at the lack of full disclosure by victims. The participants explained that this difficulty occurs when victims only show police officers some of the messages they have received from cyberstalkers. Hence PO3 in his extract was frustrated at victims who provide an incomplete evidential account because, it can lead to cases being dropped. Once again, PO3 observed that this issue was very frequent in domestic violence cases.

PO3: “We face the problem of taking the victims words against the stalkers words in court. There must be an easier way of processing the Also, victims only show some of the messages they have received thereby giving an incomplete account for investigative purposes. How can you only show half of the message and not give the police officers the full picture? They then get surprised when the case is thrown out of court. In domestic violence cases it is common for the victims to be selective of the messages that they show to the police officers. Everyone is guilty in this sense of frustrating the investigative process. They should be more aware of the impact of their conduct which could result especially in domestic violence cases in cases being dropped”.

While discussing how the behaviour of the victims can lead to lack of evidential disclosure, the participants shared the perception that sometimes, victims withhold evidential materials from police officers that link offenders to offences. Hence, Like PO3 and PO17, PRO29 expressed frustration at the lack of full evidential disclosure by some victims.

PRO29 in his extract, powerfully illustrates the frustration of the participants;
PRO29: “An additional major issue that I can think of is lack of full evidential disclosure by victims who do not paint an accurate picture of cyberstalking incidents. It is disappointing because this problem makes it difficult for police officers to gather the evidence that is required by prosecutors to prove that there is a realistic prospect of convicting a cyberstalker. The problem of lack of full disclosure by victims or victims withholding evidence is equally annoying because it can lead to cases being lost and cyberstalkers not being charged with suitable offences”.

Similarly, while discussing the behaviour of some victims in domestic violence cases, the participants shared the perception that sometimes, victims change their minds, withdraw their allegations and take the cyberstalkers back as partners thereby impeding investigation processes. PO9, therefore expressed the frustration that “some victims may become selective of the information that they provide to the police”;

PO9: “In some cases victims turn around and inform police officers that they have changed their minds. They may become selective of the information that they provide to the police. This approach undermines the time that have been invested by police officers into prosecuting cyberstalkers. It is annoying if cases are lost due to the behaviours of victims because they put in a lot of time into the investigation and prosecution of offenders”.

The participants also expressed frustration at victims who are reluctant to report incidents because of their perceived of lack confidence in the police. Hence, PO1 in his extract, asserts that there needs to be a change in cultural attitude to ensure that cyberstalking is taken seriously. The participants revealed that victims not making formal complaints can result in missed opportunities to bring cyberstalkers to justice. In this extract, PO1 discusses why victims may be reluctant to report cyberstalking incidents and the consequences of their decisions;

Int: In your opinion, why do you think that the victims of cyberstalking feel reluctant to report the conduct to the police?
PO1: “Because they feel that they will not be believed by the authorities or the police officers. Let’s say a victim of cyberstalking attends a police station to make a complaint about malicious online messages that she has been receiving from a cyberstalker and then apologises for wasting police time because she feels that the conduct she is complaining of is not serious, a weak police officer will feed off the victim’s reluctance to pursue the complainant by failing to investigate it. Such behaviours of victims will lead to missed opportunities to charge offenders and bring them to justice”.

Like PO1, and PO7, PO18 shared the perception that at the time of the study, there was a fear of getting involved with the police. The tone of PO18’s extract echoes this concern;

PO18: “Victims not having confidence in the police. Some of them feel that cases will still be dropped even if they testify. The issue of lack of confidence in the police can hinder the investigation and prosecution of cyberstalkers if offences are not reported by victims. If victims do not make formal complaints against cyberstalkers, the cyberstalkers will continue to offend”.

The participants expressed further frustration at victims refusing to attend court. Notably, PO13 explained that the reason for this issue is because some victims do not want to go through the perceived stress of appearing in court. Furthermore, PO13 uses the phrase “kick in the teeth” to describe the effect on police officers, of cases being dropped because victims refuse to testify in court

PO13: “Victims refusing to go through the stress of trials. Also, victims who have been romantically linked to cyberstalkers may refuse to testify against them in court”.

Int: Why do you feel that victims of cyberstalking are reluctant to support the prosecution of cyberstalkers?

PO13: “In some domestic violence cases, the refusal is usually because victims want to rekindle their relationships with suspects. Because there are currently insufficient trained staff to investigate such cases in some police forces, when
police officers like invest time in the investigation of cases, it is a kick in the teeth if cases cannot go ahead because victims are refusing to testify in court”.

In common with PO13, discusses how the behaviour of victims can lead to evidential difficulties, the prosecutors shared the perception that in domestic violence cases, it is difficult to obtain evidence from victims if the victims still want to maintain a relationship with the cyberstalkers. PO21 in his extract, echoed the frustration of the participants;

PO21: “We generally face several obstacles because offence is committed in the virtual world. When dealing with victims who have been in a prior relationship with the cyberstalkers it can be tasking for police officers because we find ourselves dealing with victims who are withholding evidence from the police because they want still want to have a relationship with the cyberstalkers. Dealing with such cases can be challenging for all those seeking to bring offenders to justice”.

Another aspect of victim behaviour which was discussed by the participants is that sometimes, victims cross communicate with cyberstalkers thereby, giving them mixed messages. PO17 in his extract, powerfully illustrated the frustration of the participants concerning this issue;

PO17: “Sometimes, victims give mixed messages and respond lovingly to some of a cyberstalker’s message which might result in the solicitors of a cyberstalker arguing that the victim was encouraging the cyberstalker and is only bringing a subsequent prosecution out of spite. I must admit that it is frustrating when victims cross communicate with offenders because it enables the solicitors of a cyberstalker to argue that the victim was encouraging the cyberstalker’s actions”.

Int: In your opinion, why is it a problem for victims to cross communicate with cyberstalkers?

PO17: “It could waste the time of police officers and prosecutors when victims subsequently decide to withdraw allegations just after cross communicating with victims.
In summary, the above observations highlight the shared perceptions of the participants on how victim behaviour hinders police officers and prosecutors from bringing cyberstalkers to justice. This is supported by the data in Table 4.14 which indicates that the police officers and prosecutors all identified – often in agreement the various aspects of victim behaviour that frustrate the process of bringing cyberstalkers to justice successfully.

4.4 Conclusion

This thesis reports on a qualitative study of London police officers and prosecutors perceptions of cyberstalking and the threshold of acceptable behaviour on the internet. The aim of the study was to describe the perceptions of London police officers and prosecutors on the impediments that hinder them from investigating and prosecuting cyberstalkers in London. The findings identified seven main themes:

- Threshold of acceptable online behaviour
- Legislation
- Lack of knowledge and training
- Lack of resources
- Risk assessment challenges
- Evidential Challenges
- Victim Behaviour

These key themes will be discussed in the following chapter and recommendations will be made as to how police officers and prosecutors may circumvent the issues raised in the future.
Chapter 5  Discussion, Recommendations and Conclusions:

This chapter will summarise and discuss the findings of this research for the purpose of informing recommendations. The summation highlights the objectives of the study, the primary findings and how these answered the research questions. Further, the summation identifies the general conclusions based on these findings. Additionally, this chapter highlights the limitations of the study, its theoretical implications and relationship to previous research and finally will provide suggestions for future research into the prosecution of cyberstalkers. This chapter concludes with recommendations for three groups of stakeholders in the law sector enforcement namely, the MET, the CPS and the government.

5.1 Introduction and overview of the results:

The overarching aims of the current research were threefold; firstly, to investigate how lack of resources and lack of staff training as perceived by police officers and prosecutors in London can frustrate them in the investigation and prosecution of cyberstalkers. Secondly, to discern what proactive measures are taken by police officers and prosecutors to acquire the knowledge which the participants themselves perceived to be lacking in the investigation and prosecution of cyberstalkers and thirdly what investigative impediments exist to the risk assessment of victims of cyberstalking as perceived by participant police officers and prosecutors. This research is significant given the devastating impact of cyberstalking on victims.
The unique features of cyberstalking enable cyberstalkers to harass victims instantaneously and cheaply. Goodno acknowledges that law enforcement difficulties can hinder the prosecution of cyberstalkers. From a psychological perspective, Hazlewood and Koon-Magnin emphasise that cyberstalking can create feelings of fear, terror, stress and anxiety among victims. Further, Hazlewood and Koon-Magnin stress that cyberstalkers can contact victims from any jurisdiction leading to victims living in a state of fear, terror, stress, anxiety or intimidation.

Qualitative methods were used to elicit the data and explore the research aims. Interviews were carried out with serving police officers and members of the Crown Prosecution service. The police officers and prosecutors who took part in the study, shared various perceptions on cyberstalking and what might constitute the threshold of acceptable behaviour on the internet. Although the police officers and the prosecutors provided their opinions from investigative and prosecutorial perspectives respectively, they shared common views on the issues that hinder the successful investigation and prosecution of cyberstalkers. Interviews were analysed using Thematic Analysis. 7 main themes emerged from the data; (threshold of acceptable online behaviour, legislative issues, lack of training and knowledge, lack of resources, risk assessment challenges, evidential challenges and victim behaviour) and the findings of these are discussed in the sub sections that follow.

---

515 ibid
516 Virginia Braun and Victoria Clarke ‘Using Thematic Analysis in Psychology’ (2006) 3 Qualitative Research in Psychology 7
5.2 Threshold of acceptable online behaviour and how it is distinguished from cyberstalking:

Given that the internet enables cyberstalkers to communicate anonymously, the threshold of acceptable behaviour online ought to be established to encourage internet users to conduct themselves in a law abiding manner when interacting with others on the internet.\textsuperscript{517} The responses of the participants on the threshold of acceptable online behaviour are therefore insightful because their responses identify various thresholds as determined by the participants through their own professional experience. The findings relating to this theme revealed that both prosecutors and police officers perceived that a level of objectivity is required in determining when the threshold has been crossed (PO6, PRO19 and PO23: Chapter 4, pages 196 and 197). For example, application of the objectivity test can be used in order to determine whether the actions of a mentally ill individual who is accused of cyberstalking do indeed constitute harassment. This principle has previously been explored by PRO 28 in the case of \textit{R v Colohan} wherein the accused’s defence on the basis of mental ill health was ruled irrelevant based on the premise that the question that should be asked is whether any reasonable person would consider that the actions of the individual amount to harassment (PRO 28: Chapter 4, page 198).\textsuperscript{518} It is important to note that although the investigation of mentally ill cyberstalkers was raised in brief in the data, this thesis does not investigate the challenges faced by police officers in the investigation and prosecution of mentally ill cyberstalkers.

\textsuperscript{517} This is more so because, as previously highlighted, cyberstalking can result in either the murder or suicide of victims

\textsuperscript{518} [2001] AllER 230
The participants also, discussed where the impact of cyberstalking on victims falls in relation to the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking (PROB: Chapter 4, pages 192 and 193). They maintained that the yardstick should be whether victims expressed distress and alarm as a result of the behaviours. It is important to note that in expressing the above view, the participants made a distinction between cyberstalking and face to face stalking as highlighted (PO8, PO12 and PO19: Chapter 4, pages 192 and 195.)\textsuperscript{519}

However, it was also argued that a cyberstalker may be unaware of the impact that his conduct has had on a victim because unlike face to face stalking, it is hard to judge the immediate reaction of a victim and in some instances offenders realize that they have committed an offence only after they have been questioned by police officers (PO12, PO19 and PO25: Chapter 4, pages 194 and 195).

In contrast to the above, participants referred to the case of R v Blaue and stressed that the threshold will depend on whether the cyberstalker sought out a vulnerable victim (Chapter 4: page 199). Notably, from a legal perspective, the participants asserted that the principle established in this case weakens the argument that sometimes cyberstalkers lack the required intention to commit offences. The legal principle established in the case of R v Blaue, stipulates that offenders are legally required to take their victims as they find them.\textsuperscript{520} Therefore, applying this legal principle to cyberstalking cases, it follows that if certain victims are suffering from pre-existing health conditions which worsen after they have been harassed by cyberstalkers, they may be unaware of the impact their conduct has had on them.

\textsuperscript{519} The participants stated that cyberstalkers may be unaware of the impact if their behaviour on victims because they communicate with victims in the cyber realm as opposed to stalkers in the physical realm who are able to gauge the reaction of victims.

\textsuperscript{520} [1975] 1 W.L.R 1411
cyberstalkers, the cyberstalkers will be liable for the subsequent deterioration of their health even if the cyberstalkers are unaware of the health conditions and the impact of their actions on the health of such victims.\textsuperscript{521}.

While discussing the threshold and the right to freedom of expression, a participant prosecutor explained that because the internet is full of people with opinions, the right to freedom of expression should be respected provided a crime has not been committed (Chapter 4: page 199). However, it can be argued that there is a fine line between freedom of speech and the right to privacy in the cyber realm which by definition is designed to have worldwide publication. Hence, it can be inferred that the intention of the cyberstalker who posted the messages will determine the threshold. This thesis argues that a cyberstalker’s right to freedom of expression should be balanced against a victim’s right to privacy despite the inferred intention of the cyberstalker.

Furthermore, participants suggested that the size of the electronic platform from which a cyberstalker disseminated messages might indicate the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking. They argued that if the platform is small, private and limited to a small audience then this could be deemed less harmful (Chapter 4: page 204). This thesis does not accept this view given that victims can be affected if they are targeted by cyberstalkers who have posted messages on private settings despite the fact that the audience may be smaller in comparison to the audience of a cyberstalker who posts offensive messages on a public setting as the level of harm is surely relative to the individual affected?

\textsuperscript{521} Therefore, a cyberstalker’s ignorance on the impact of his conduct on a victim will not be construed as a defence by the courts
In relation to this theme, around one third of participants revealed they would refer to legislation to assist their decision although this might prove challenging to establish the threshold via reference to for example the Protection from Harassment Act (PHA) because the PHA does not expressly define cyberstalking as a specific offence.\textsuperscript{522} For a conduct to constitute cyberstalking, it has to satisfy the legislative requirement stipulated by section 7 of the PHA ‘\textit{that a conduct has to occur on more than one occasion}’.\textsuperscript{523}

Likewise, the gravity of an offence might be useful in determining the threshold especially if the offence escalates to violence being used. However, it is important to note that the threshold will only be crossed when a behaviour becomes menacing because mere rudeness is not actionable. Therefore the behaviour will need to be in the nature of racism, libel, homophobia or malicious intent. This view implies that certain acts will be considered by police and prosecutors as offences if they are linked to traditional defamatory offences. The research’s stance on this issue is that an offensive or threatening behaviour will result in a victim experiencing alarm, distress or the fear of violence which constitute stalking offences as defined under section 2A and 4A of the PHA. The offences were previously discussed in Chapter 2, sections 2.3.3 and 2.3.4.

In conclusion, previously discussed research findings reveal that victims are affected by the activities of cyberstalkers. Notably, in a recent study which was conducted in

\textsuperscript{522} Instead s2A (3) b, c, d f and g of the PHA list statutory examples of the activities of cyberstalkers. These aspects of the legislation govern the criminal activities of a cyberstalker ranging from the publishing of statements by any means in the name of another person to the monitoring of an individual’s internet usage.

\textsuperscript{523} This feeling was echoed by another prosecutor who went further to state that if a conduct occurs on more than one occasion, it will constitute cyberstalking.
the year 2019, Maran and Begotti found that victims suffered from depression and traits of anxiety in comparison to non-victims. Maran and Begotti therefore highlight the importance of preventing cyberstalking and offering support to victims of cyberstalking. Likewise, Worsley, Wheatcroft, Short, and others thematically analysed the experiences of one hundred victim narratives via an online survey in order to assess the mental health and well-being implications of the experience of cyberstalking. Worsley, Wheatcroft, Short, and others found that the emotional impact of cyberstalking primarily includes comorbid anxiety and depression. Notably, they found that cyberstalking can affect the psychological, social, interpersonal, and economic aspects of the lives of victims. Additionally, they found that victims adopted various coping measures which include making major changes to both their work and social life, stopping employment and changing usual daily activities.

In light of the above, the majority of the participants in this study shared the perception that there are different thresholds for distinguishing between rudeness, abuse and unpleasant comments on the internet and cyberstalking some of these being victim specific.

524 Daniela Maran and Tatiana Begotti ‘Prevalence of Cyberstalking and Previous Offline Victimization in a Sample of Italian University Students’ (2019) 8 Soc Sci 1
525 Maran and Begotti compared the effects of cyberstalking between victims of cyberstalking and victims of cyberstalking and previous offline victimization in their lifetimes based on a sample of 229 Italian students who completed a self-administered questionnaire
5.3 Legislation and law enforcement issues

5.3.1 Legislative difficulties

The participants shared the perception that there is no single legislation expressly criminalising cyberstalking in the UK. (PO9, PO12, PO24 and PRO25: Chapter 4, pages 214 and 215). The need for an effective legal structure to address the criminal behaviour of cyberstalking was discussed by Basu who argues that the legal system is not structured to deal with criminal offences perpetrated in the virtual world.\(^{527}\) Hence, Geach and Haralambous argue that in the information and technology sector, criminalising a conduct that is specific to online acts may be problematic if due to technological advancement, a particular technology becomes so outdated that it no longer matches the technology as specified in an offence.\(^{528}\) Geach and Haralambous therefore suggest that to fulfil the principle that the law is certain, the legislation should provide a clear and precise definition of cyberstalking.\(^{529}\)

Similarly, the fact that there is no acceptable definition of cyberstalking has been acknowledged.\(^{530}\) Vasiu and Vasiu stress that cyberstalking can have psychological, economic or physical effects on victims and can result in the perpetration of violent crimes. They emphasise that it is a challenge to define cyberstalking.\(^{531}\) Likewise, Chick argues that cyberstalking differs from stalking in the physical realm.\(^{532}\)


\(^{528}\) It is contended that in such situation, the technology develops into something that no longer matches, what is defined in the offence.

\(^{529}\) Neal Geach and Nicola Haralambous, ‘Regulating Online Harassment: Is the Law Fit for the Social Networking Age?’ (2009) 73 (3) Journal of Criminal Law 3


\(^{531}\) Suzanne Van der Aa, ‘International (Cyber) Stalking, Impediments to Investigation and Prosecution’ (Pure, 2011) <www.pure.uvt.nl/ws/files/1310512/Aa_International_cyberstalking_110216_posprint_embargo_1.pdf> accessed 9 August 2018

asserts that the difference can be attributed to communication, jurisdictional and evidential factors.

The significance of legislative difficulty is two dimensional. From the first dimension, it highlights that UK police officers will have no legal standing and will be unable to establish that a cyberstalker has committed an offence in the UK which is similar to an offence in a foreign country if cyberstalking is not a proscribed conduct in the foreign country in which the cyberstalker resides. From the second dimension, it indicates that if cyberstalking has not been criminalised in the foreign country, the UK police officers will be unable to utilize extradition as a method of international cooperation. This is because, the international officials in the foreign country may use the fact that cyberstalking is not a proscribed conduct as a ground for refusing the extradition of a cyberstalker. From a law enforcement perspective, the implication of the legislative difficulties is that law enforcement officials may find it challenging to initiate legal actions against cybercriminals if countries have not enacted laws criminalizing the conduct that perpetrators engage in.  

From an extradition perspective, when investigating a case where a cyberstalker and the victim reside in different jurisdictions, UK police officers and prosecutors face the related difficulty of identifying which jurisdictional law will be applicable to a given case. This is because the law enforcement authorities in a cyberstalker’s country of residence could refuse to extradite a suspect on the grounds that they do not extradite nationals. Consequently, Shearer argues that some international extradition treaties may contain either mandatory or discretionary bars to the extradition of nationals.

---

exempting countries from extraditing citizens.\textsuperscript{534} Shearer suggests that there is no moral duty on countries to extradite a fugitive in the absence of an extradition treaty.

The findings indicate that the despite the above criticisms, some of the participants acknowledged that the amended Protection from Harassment Act is an important tool for regulating cyberstalkers with a view to successfully bringing offenders to justice. Figure 5.3.1 below illustrates the relationship of the various legislative difficulties identified by participants

Figure 5.3.1 Legislative Difficulties perceived by participants.

Given the various background experiences of the participants, the view of criminalising cyberstalking as an aspect of cybercrime were varied. Importantly consensus of agreement amongst prosecutors and police officers was high (>90%), concerning the

legislative issues which frustrate them such as the issues of restraining orders being breached by cyberstalkers and the need to establish a course of conduct under the PHA.

The participants were not convinced of the efficacy of the existing legislation pertaining to cyberstalking particularly as some victims do not report incidents when they occur. Hence, Alghrim emphasises that cyberstalking is a relatively new phenomenon and argues that cyberstalking is likely to be underreported due to limited knowledge of what behaviours constitute cyberstalking. Importantly, Alghrim stresses that there are many factors unique to cyberstalking which may affect the extent to which the offence is reported, and the extent to which the offender or victim is held accountable.

Furthermore, in the current research, Police officers and Prosecutors shared the perception that lenient sentencing under the PHA was an issue. The participants were of the opinion that cyberstalkers should be given stronger sentences to deter future offenders (PO16 and PO23: Chapter 4, page 212). The participants indicated that tougher sentencing options should be provided because there is a commonly held perception that the criminal justice system is lenient on offenders and that victims instead, are given a tough time (See chapter 2 sections 2.3.3 and 2.3.4). It is important to note that this aspect of legislative concern was acknowledged by the government on 17 September 2019 when the Ministry of Justice announced that the government will allow victims of criminals convicted of stalking, harassment, child abuse and other sex offences to argue for offender sentences to be increased if victims or the public

think their original punishment was too lenient.\textsuperscript{536} This recent change justifies the frustration of the participants who at the time of the interviews expressed the view that the sentences that are given to some cyberstalkers are too lenient. The thesis revealed this issue prior to the government announcement and therefore it can be construed that this subsequent change in sentencing provides support for the findings in this thesis.

Additionally, it was revealed that it may be difficult to prove that a cyberstalker’s behaviour amounted to a course of conduct as defined under s7 of the PHA as previously discussed in Chapter 2, Section 2.3.11.\textsuperscript{537} This is further complicated because there is no specific legislation in the UK that criminalizes cyberstalking because there was no specific offence of cyberstalking that existed at the time the interviews took place. The police officers emphasised that instead, there are different pieces of legislation which criminalize different aspects of the conduct.

From a legislative perspective, the participants stated that it may be difficult to prove a course of conduct under the PHA (PO18 and PRO26: Chapter 4, page 218). This is because, in comparison to the MCA, sections 2 and 2A of the PHA respectively, stipulate that the offences of harassment and stalking respectively will be committed if there is a conduct which amounts to harassment and that particular harassment constitutes a stalking behaviour. This demonstrates that if a cyberstalker disseminates a rude, abusive, offensive or threatening communication on one occasion then the offender will be prosecuted under the section 1 of the MCA. Whereas, if a cyberstalker


\textsuperscript{537} Section 7 of the PHA defines a course of conduct as occurring on at least two occasions
embarks on a more intense campaign of harassment for a longer duration and on more than one occasion, the cyberstalker will be prosecuted under the PHA.

From a prosecutorial perspective, the participants also highlighted the issue of victims reporting offences outside the statutory time limit. This issue can be linked to delay in report by victims. Hence while discussing the related issue of underreporting, Oltman argues that victims underreport crimes for various reasons ranging from not wanting to bother the police to feeling embarrassed. Additionally, Oltman states that the consequences of victims not reporting crimes are lack of accurate data about crime in communities which results in more risk to citizens and resource allocation not being effectively deployed to tackle the criminals. In light of these observation and given that the statutory time limit for bringing offences under the s 2 of the PHA is 6 months, the researcher argues that there is an onus on police officers to effectively explain to the victims, the statutory requirements for proving offences under the PHA to ensure that they promptly report offences and meet the legislative criteria for proving that an offence has been committed.

From a statistical perspective, in 2017 the Office for National Statistics published a report ‘Reasons for Not Reporting Crime to the Police in England and Wales’. The statistical data provided 17 reasons why victims do not report offences. Notably, 3 of the reasons reflected the perception of the participants in this research these were; i) the perception that an offence is too trivial ii) the perception that police officers will not be bothered to investigate offences and most importantly iii) the fear of reprisal.

---

This report once again provides support for the findings of this thesis as this reason was highlighted by a participant when explaining why victims refuse to testify against cyberstalkers in court. Furthermore, in respect of points i) and ii) above, a prosecutor expressed the view that if police officers do not take cyberstalking incidents seriously, they will miss opportunities to bring offenders to justice.

The research also revealed the frustration of participants with persistent cyberstalkers who breach restraining orders thereby jeopardizing the safety of victims. Hence to ensure that victims of stalking and harassment are adequately protected, in their 2017 report, Her Majesty’s Inspectorate of Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate stated that there should be a proper examination of persistent offending, instead of an assumption that breaches of restraining orders will be prosecuted ahead of major crimes.\textsuperscript{540}

Despite the above legislative criticisms, the researcher is aware that in the UK, an additional attempt is being made to further criminalise stalking and cyberstalking implicitly via the Stalking Protection Order which is a civil order. Hence, on 23 November 2018, it was reported that the Stalking Protection Bill, sponsored by Dr Sarah Wollaston MP, had its third reading in parliament.\textsuperscript{541} The bill which was backed by the government received Royal Assent on 15 March 2019.\textsuperscript{542} It is anticipated that the bill will introduce Stalking Protection Orders to improve the safety of stalking

\textsuperscript{541} ‘What is Stalking Protection Orders’ (Suzylamplugh, 2016) <https://www.suzylamplugh.org/what-is-the-stalking-protection-bill> accessed 29 April 2019
victims giving police the authority to tackle the danger that perpetrators pose while they gather more evidence and deal with particular issues related to the crime. More importantly, the Stalking Protection Orders may require stalkers and cyberstalkers implicitly to be psychologically assessed or to attend rehabilitation programmes to help prevent reoffending. From a mental health perspective, this development is significant given that some of the participants expressed frustration at investigative challenges which hinder the prosecution of mentally ill cyberstalkers (see Chapter 4 Section 4.3.6).

In light of the above, the majority of the participants in this study shared the perception that various legislative difficulties frustrate them in the investigation and prosecution of cyberstalkers.

5.3.2. Lack of knowledge and training:

Lack of knowledge and training was a principal theme identified in the study by the majority of the participants (> 93%). Given that the participants shared several frustrations regarding the sensitive issue of lack of training and knowledge, the researcher recognized that issues of research bias could prevent participants from providing detailed responses due to a fear of losing their jobs. Therefore, Pannucci and Wilkins acknowledge that research bias can occur in planning, data collection and the analysis phase of research. Likewise, Smith and Noble highlight that bias can

543 ibid
544 ibid
545 Christopher Pannucci and Edwin Wilkins ‘Identifying and Avoiding Bias in Research’ (NCBI, August 2010

303
occur at different stages of the research. The issue of bias was previously discussed in chapter 3, section 3.1.1.

The researcher was aware that because of the sensitivity of the topic, the participants may not be forthcoming with information. Holt, Bossler and Fitzgerald in explaining low response rates among specific law enforcement research participants, highlighted that participants may have had some reservations over proffering information on behalf of their organizations on matters relating to training and caseloads. Further, Sleath and Bull emphasise that it may be difficult to recruit meaningful samples of police officers especially if the research topic is sensitive. Consequently, the researcher was rigorous in implementing strategies (See Chapter 3) at each interview to ensure that the participants felt confident in the research protocols in place whilst they disclosed information relating to lack of training and knowledge in respect of the following four aspects: police officers, ISPs, the judiciary and members of the public. The key sub-themes that emerged from the interview data are shown in Figures 5.2 and 5.3:

548 Emma Sleath and Ray Bull ‘Comparing Rape Victim And Perpetrator Blaming In A Police Officer Sample’ (2012) 39 Criminal Justice and Behaviour 5
Figure 5.3. 2 Lack of Knowledge issues identified by participants

- Risk assessing victims and offenders
- Legislation
- Lack of knowledge
- How to track and unveil the identities of anonymous cyberstalkers
- Police knowledge on CPS evidential thresholds
- Importance of providing evidence once a suspect has been charged
- Connecting cyberstalkers to unregistered sim cards

Figure 5.3 Lack of Training issues identified by participants

- Lack of training
- Assessing digital evidence
- Gathering and preserving digital evidence
- Psychological impact of cyberstalking on victims
- Obtaining computer and phone evidence
- IP and email addresses
- Risk assessment of victims and cyberstalkers
Shan highlights that Scotland’s first national prosecutor for domestic abuse has emphasized that police officers require additional training in tackling stalking and cyberstalking implicitly to ensure successful prosecutions.\textsuperscript{549} The issue of lack of police knowledge on the investigation of stalkers and implicitly, cyberstalkers was discussed by Lynche and Logan who investigated two groups of police officers on perceived barriers to charging and attitudes relating to charging stalking offences.\textsuperscript{550} Importantly, their results demonstrated that officers who had never investigated stalking, found the offence less dangerous, did not file relevant reports on reported incidents and perceived barriers related to charging stalking more challenging than police officers who had investigated stalking before.\textsuperscript{551} The study found that police officers who had previously investigated stalking, had a greater understanding and were able to identify specific statutory problems. The findings of their research is arguably relevant to cyberstalking which is an aspect of stalking.

Lack of knowledge on the extent and nature of cyberstalking can lead to police officers under recording stalking and cyberstalking offences implicitly compared to other offences and perpetrators being arrested for them. Consequently, Brady and Nobles examined police officers response to stalking at a Houston police station to investigate the issue of underreporting and under recording of stalking incidents.\textsuperscript{552} Brady and Nobles examined 3,756 stalking incident calls and stalking calls for service which

\textsuperscript{549} Ross Shan ‘Stalkers Freed due to lack of Police Training’ (The Scotsman, 10 February 2014)
\textsuperscript{550} Kellie Lynch and TK Logan ‘Police Officers Attitudes and Challenges with Stalking’ (2015) 30 Violence and Victim 6
\textsuperscript{551} ibd
\textsuperscript{552} Patrick Brady and Matt Nobles ‘The Dark Figure of Stalking: Examining Law Enforcement Response’ (2017) 32 Journal of Interpersonal Violence 20
had occurred over 8 years and found that that there were only 66 stalking-related incident reports, and only 12 arrests for stalking. Worryingly, Brady and Nobles also found that not one of the stalking calls for service generated a stalking-related incident report nor led to an arrest for stalking. Additionally, Brady and Nobles found that the majority of the stalking calls for service which generated an incident report were classified as harassment or a protective order. Importantly, Brady and Nobles revealed that incident reports and arrests for stalking generally arose regarding harassment or terrorist type threats.

Likewise, a report which was conducted by HM Crown Prosecution Service Inspectorate and Her Majesty’s Inspectorate of Constabulary into how the police and CPS respond to stalking and harassment made crucial findings. The report found that lack of understanding of what constitutes stalking manifests in the under recording of stalking offences, and the wide variation of recorded stalking offences between police forces. The report additionally emphasised the issues of stalking being wrongly identified as harassment, police officers not properly understanding the nature of the offending and the risks to the victim and subsequently investigations not being allocated to specially trained officers. From a victimisation perspective, the report stressed that if stalking and cyberstalking implicitly are wrongly identified as harassment, it could result in victims not being referred to specialist stalking support services when available.

The difficulty posed by lack of training was highlighted by the participants in the current research from the following three perspectives: insufficient trained officials, lack of public awareness on cyberstalking and the lack of trained computer experts to assist police officers in the investigation of cyberstalkers.

On 5 July 2017, subsequent to the completion of the interviews carried out for the current research, Her Majesty’s Inspectorate Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate published critical findings of their joint inspection into how the MET and the CPS tackle the offences of harassment and stalking offences.\textsuperscript{555} The findings highlight that the CPS and the MET are required to implement additional measures with a view to ensuring that all lawyers and prosecutors have received training in harassment and stalking. The inspectorates anticipated that ensuring that lawyers and prosecutors receive the training will lead to improvements in the prosecution of harassment and stalking offences.\textsuperscript{556} Particularly, the inspectorates recommended that the CPS provides training for prosecutors in terms of professional development and awareness-raising in an informal environment.

The findings of the inspectorates reflect similar issues to those raised by the participants, that prosecutors lack implicit knowledge of stalking and cyberstalking offences and therefore require training.\textsuperscript{557} Furthermore, the findings of the current research revealed a shared frustration that police officers also lacked the requisite knowledge on how to trace the emails or internet portal addresses of suspects. The participants were of the view that all police officers ranging from the lowest ranks to

\textsuperscript{555} CPS Response to HMIC/HMCPSI Joint Thematic Inspection of Harassment and Stalking Offences’ (CPS, 2017) \<www.cps.gov.uk/publications/docs/cpsresponse to hmic hmcpsi harassment stalking report, pdf > accessed 2 December 2019

\textsuperscript{556} ibid

\textsuperscript{557} The inspection of Her Majesty’s Inspectorate Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate into how the MET and the CPS tackle the offences of harassment and stalking offences
the most senior require training in the technological elements of computer forensics for investigating cyber-crimes. The researcher acknowledges that at the time this study was concluding, the CPS had introduced the *Stalking and Harassment* package of training measures for prosecutors.

A further implication of this lack of training is that police officers are prevented from accessing, obtaining and preserving the digital evidence that they need to successfully prosecute these perpetrators through lack of technological knowledge. This also has a negative impact on evidential clarity as without the requisite knowledge to gather evidence effectively from the internet the result can be police officers implementing inconsistent measures. Therefore this thesis asserts that basic training in these necessary skills should be mandatory for officers of all ranks.

The interview data also revealed a further crucial shortfall in knowledge relating to the psychological impact of cyberstalking on victims. Confirming this, one participant prosecutor reiterated that there was a dangerous misconception that because cyberstalking is not physical, it is less serious. On this basis it could be construed that such a misconception can prevent law enforcement officials from appreciating the severity of certain cyberstalking offences especially in domestic violence cases and cases involving the victimisation of vulnerable children.

Additionally, the findings revealed a vital shortfall in knowledge relating to the misconception that cyberstalking is not as serious as face to face stalking because cyberstalking occurs in the cyber realm. Maran and Begotti recently compared the effects of cyberstalking between victims of cyberstalking and victims of cyberstalking
and previous offline victimization in their lifetimes. They hypothesised that cyberstalking had an impact on the wellbeing of victims and contributed to increases in physical and emotional symptoms, anxiety and depression, and that those symptoms increased in victims who had suffered previous offline victimisation. Maran and Begotti’s study was based on a sample of 229 Italian students who completed a self-administered questionnaire. The study found that in general, the prevalence of cyberstalking in the study sample was higher than in previous investigations. With regard to consequences, victims indicated higher scores for depression and anxiety than non-victims. From a risk assessment perspective, the study was significant because it highlighted that victims can be subjected to both cyberstalking and face to face stalking. Additionally, the study highlighted the importance of preventing cyberstalking and recommended that victims of cyberstalking are offered support.

Further shortfalls in police knowledge were also revealed in relation to risk assessment. The police participants identified that they lacked knowledge on how to risk assess anonymous cyberstalkers and that as a result of this issue police officers are hindered from protecting victims. However, it should be acknowledged that one participant who had previously worked in the Serious Organised Crime Agency, (which is now defunct), had been in receipt of specialist training due to the nature of his job. The police officer confirmed that although he himself had received training on the core investigative skills that police officers require to investigate internet crimes, non-specialist-police officers had not received the same training.

559 Ibid
560 In doing so, the police officer indicated that he had received specialist training which enabled him to investigate digital enabled crimes such as phishing and online blackmail
561 The police officer, was of the view that the implication is that non-specialist police officers will not be able to retrieve the required evidence in situations for example when victims drop their mobile phones in the bath and lose relevant evidence
Shortfalls in knowledge in respect of the identification of cyberstalkers suffering from mental ill health were also revealed to have a detrimental impact on the risk assessment process, particularly if at the time of arrest they did not display overt signs of mental illness. Crucially, the findings reveal that this lack of knowledge prevents police officers from establishing when suspects who have been arrested require medical treatment.

In summary, it is clear from this theme that participants from both professions share the view that successful investigation and prosecution of cyberstalkers is hampered through lack of knowledge and training in the key staff involved. However, the findings also revealed that participants have relied upon a wide range of alternative measures including personal research, liaising with colleagues, learning on the job, reading up on materials to widen their professional knowledge and fill gaps in the skills they require. It is also notable that subsequent to the conclusion of this research the relevant authorities have recognised the need for a package of training measures to supplement knowledge in this area. This thesis now argues that this package is made mandatory for all officers and legal professionals involved in this field.

3.3 Lack of resources

‘Lack of resources’ was the fourth main theme identified in the study by the majority of participants as a factor that frustrates police officers in the investigation and prosecution of cyberstalkers.
Once again the researcher was aware that due to the working relationship between her and the participants, the participants may be reluctant to fully divulge certain aspects of the perceived issue of lack of resources that frustrates them in the investigation and prosecution of cyberstalkers. The researcher was also aware of the risk that research bias could prevent the participants from expressing their views in detail on the perceived issue of lack of resources due to a fear of disciplinary repercussions. The researcher was especially aware that bias could arise when the perceived issues of the allocation of heavy caseloads and staff shortages were being discussed by the participants. Therefore, as before the researcher was rigorous in ensuring that when conducting interviews she was not perceived as controlling and she actively sought to maintain a balance of power between herself and the participants.

The findings indicate that the participants identified six perceived resource issues which frustrate them in the investigation and prosecution of cyberstalkers. The relationship of these issues is shown in Figure 5.3.3:
In summary, the legislative difficulties shown in Figure 5.3.3., represent the issues perceived by participants which impede the investigation of cyberstalkers. It is important to note that the study found that in some cases, there is a relationship between the issue of lack of resources and the inability of police officers to risk assess victims and perpetrators.

The findings reveal that police officers and prosecutors shared frustration at the lack of a single point of contact to enable the participants to liaise with the correct officials from the beginning to the end of cases. The researcher is aware that in reality, the national stalking protocol requires each police force and CPS Area to appoint a single point of contact (SPOC) for stalking to enhance effective and early consultation.
between the police and the CPS. The researcher further acknowledges that on 5th July 2017, Her Majesty’s Inspectorate Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate in their critical joint findings, highlighted that the SPOC should include close liaison with third-sector organisations that provide support to victims of stalking and cyberstalking implicitly.

Importantly, the findings of the current research suggest that lack of manpower results in missed opportunities to risk assess both victims and cyberstalkers due to the allocation of heavy caseloads. This also might prevent officers recognising that an offence is actually taking place. Consequently, from a domestic violence perspective, the dangers associated with missed opportunities to risk assess cyberstalking victims in such cases was also highlighted to present a very serious issue. This finding is worrying given that academics have stressed that victims of stalkers particularly and cyberstalkers implicitly, face various physical and mental risks from stalkers. Notably, McEwan, Pathe, James and Ogloff emphasise that clinicians ought to consider various risks ranging from the risk of physical violence towards the victim or a third party to the risk of psychological damage to the victim.

The findings suggest that due to lack of resources, cyberstalking may not be perceived as a grave offence when cases are being prioritized by over worked police officers.

---

564 The police officer further explained that an over worked police officer may fail to risk assess offenders thereby, wrongly assuming that offenders are merely showing unhealthy interests in the victims
566 ibid1
Consequently, the participants expressed the view that the issue of heavy caseloads is compounded by the fact that there is a high unrealistic public expectation for police officers to investigate all incidents of cyberstalking incidents.

The issue of lack of resources can arguably affect the ability of police officers to detect and solve offences. Coupe examined the effects of police officer resources and the ease with which crimes may be solved, on burglary detection.\textsuperscript{567} Coupe found that the application of resources to the investigation of solvable incidents helps explain detection levels and based the study on data obtained from computerised police incident logs and self-completed surveys of officers.\textsuperscript{568}

The participants shared the misgiving that there was no centralized database for gathering and accessing local intelligence on cyberstalkers and indicated that it will be a challenge for police officers in different forces to share local intelligence concerning unknown cyberstalkers due to bureaucratic processes.

Given the above observations regarding the lack of a centralized unit, the researcher acknowledges that in 2017, the CPS and the MPS introduced a Stalking Single Point of Contact in response to Her Majesty’s Inspectorate of Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate’s report on the current approach to tackling crimes of harassment and stalking.\textsuperscript{569} The inspectors recommended that the National Police Chief Counsel and the CPS stalking leads review the single point of

\textsuperscript{567} Richard Coupe ‘Evaluating the Effects of Resources and Solvability in Burglary Detection’ (2016) 26 An International Journal of Research and Policy 5

\textsuperscript{568} ibid

\textsuperscript{569} ‘CPS Response to HMIC/HMCPSI Joint Thematic Inspection of Harassment and Stalking Offence’ (CPS publications, 5 July 2017) <www.cps.gov.uk/publications/docs/cps response to hmic hmcpsi harassment stalking report> accessed 8 August 2017

315
contact system and ensure that it is completely effective and operating uniformly for victims in all areas.570 As previously discussed (Chapter 1, section 1.5), the researcher acknowledges that since the conclusion of this study, that the CPS and the National Police Chiefs’ Council have strengthened the Single Point of Contact for the investigation and prosecution of stalking offences to ensure that the Police and CPS leads on stalking fully understand the requirements and expectations of the role.571 Additionally, the researcher acknowledges that there are several charitable organizations in the UK which work with police officers when required on cyberstalking such as the Suzy Lamplugh Trust, the Protection against Stalking, the National Stalking Helpline and the Cybersmile charity among others.

In summary it is clear from this theme that participants from both professions share the view that the successful investigation and prosecution of cyberstalkers is hampered by lack of resources. More concerningly, this issue can prevent police officers from risk assessing victims. It is also notable that subsequent to the conclusion of this research, the relevant authorities have recognized that lack of resources can impede the investigation and prosecution of stalkers, lead to the allocation of heavy caseloads and result in missed opportunities to risk assess both victims and cyberstalkers.

571 As previously discussed, the measures were introduced following Her Majesty’s Inspectorate of Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate inspection and report
5.3.4 Risk assessment challenges

Given that cyberstalking can affect victims psychologically, emotionally and physically, there is an onus on police officers and prosecutors to ensure that victims are risked assessed and that identified risks are managed during the investigation and processes. The relationship between the issues raised and risk assessment of victims is illustrated in Figure 5.3.4 below:

**Figure 5.3.4 Issues that impact on Risk Assessment.**

The participants highlighted the additional importance of risk assessing the cyberstalkers given that some cyberstalkers may be mentally unwell (PRO12 and PO13 and PO21: Chapter 4, page 255). Groenen and Vervaeke emphasise that cyberstalkers should be risk assessed to ascertain if offenders have mental...
illnesses. Groenen and Vervaeke also acknowledge that academics have argued that when assessing risk to victims, the following 3 factors should be considered by police officers; i) risk of physical violence, ii) risk of the victim suffering psychological or social damage and iii) risk of the offence continuing to occur or reoccurring.

From a mental health perspective, McEwan, Pullen and Purcell stress that the stalking behaviour can lead to substantial damage in victims, whether the perpetrator is violent or not. Therefore, from a mental health perspective, they emphasise that the responsibility for assessing and managing risks lies with mental health professionals. From a law enforcement perspective, the researcher asserts that police officers also have a crucial role to play in identifying, monitoring and managing risks to victims when offenders are questioned, arrested and charged and during the investigation process. The researcher also argues that prosecutors by liaising with police officers in the progression of cases, have a role to play in ensuring that victims of cyberstalking cases are risk assessed. Hence as previously discussed (Chapter 1, section 1.3 and Chapter 2, section 2.7 respectively), the CPS and the MPS have introduced risk assessment measures to protect victims ranging from the introduction of relevant legal guidelines to the introduction of a Risk Identification and Assessment Model.

From a domestic violence perspective, the participants expressed frustration at cyberstalking victims in domestic violence cases refusing to implement recommended

575 The identified the following damage: assault, persistent stalking, recurring stalking, psychological damage and social damage
risk assessment safety measures. The responses of the participants revealed that it can be challenging for police officer to risk manage victims who have intermittent relationship with cyberstalkers. This finding is concerning, given that a study in 2019 found that stalking and cyberstalking victims (implicitly) in domestic violence cases are more likely to be targeted by offenders. The study was conducted by Bendlin and Sheridan based on a sample of 369 police incident reports into domestic violence which identified correlates of nonviolent, moderate, and severe physical violence where stalking behaviour was indicated. The incident reports that featured in the study occurred between 2013 and 2017 between intimate or ex-intimate partners.

Similarly, the CPS acknowledged, in the current annual *Violence against Women and Girls report*, that a majority of stalking and cyberstalking incidents implicitly in 2018-19 related to domestic abuse. Importantly, the CPS highlighted that the joint police and CPS protocol on stalking has equipped police officers and prosecutors with tools to better identify offending. The researcher argues that the challenge for the CPS and the MPS is to work collaboratively with a view to tackling the issue of cyberstalking victims in domestic violence cases refusing to support the prosecution of offenders given that as previously discussed (Chapter 1, section 2.2), cyberstalking can lead to the death of victims either via murder or suicide.

From a domestic violence risk assessment perspective, the CPS has published Domestic Abuse Guidelines for prosecutors which contain risk assessment checklists.

---

578 ibid
and risk assessment indicators. The risk assessment checklists and indicators will equip prosecutors with the skills that they require to identify victims of domestic violence and related cyberstalking who need to be risk assessed and risk managed. The CPS has given 3 assurances in relation to the Domestic Abuse, Stalking and Honour Based Violence risk assessment (DASH) and the stalking risk screening tool. The first assurance is that prosecutors will ensure that the DASH and the stalking risk screening tool have been applied by the police. The second assurance is that the DASH and the stalking risk screening tool will be used to inform decisions regarding bail or remand. The third assurance given by the CPS is that the DASH and the stalking risk screening tool will be used to inform safeguarding plans in relation to the victim. Notably, the CPS confirmed that in cases of domestic violence this will be in addition to the Joint CPS ACPO Domestic Violence Evidence Checklist.

Section 5 of the Protection from Harassment Act 1997 empowers criminal courts to make a restraining order after a conviction under either section 2 or section 4 of the Act. Additionally, section 12 of the Domestic Violence, Crime and Victims Act 2004 extended the power of criminal courts to impose orders for any criminal offence, and on acquittal as well as conviction. However despite these statutory provisions from a risk assessment perspective, the participants expressed frustration at cyberstalkers who breach restraining orders and continue to cyberstalk victims. The frustration is understandable given that in the ‘Protocol between the National Police Chief’s Council and the Crown Prosecution Service, the stakeholder acknowledged that breach of

581 ibid
582 It was anticipated that these statutory provisions will reduce the risk to and potential victims of stalking, domestic violence, harassment and other offences. However the effectiveness of the orders have been questioned given that some offenders persist in offending
restraining orders is evidence of further stalking and harassment offences.\textsuperscript{583} The protocol was previously discussed in Chapter 1, section 1.4. Therefore, Benitez, McNiel and Binder highlight that there is a controversy over the effectiveness of protection orders and restraining orders implicitly despite acknowledging that restraining orders can be an effective tool for threat management.\textsuperscript{584}

From a critical perspective, while addressing the issue of the breach of restraining orders by offenders in stalking harassment and cyberstalking cases implicitly, Her Majesty’s Inspectorate of Constabulary and Her Majesty's Crown Prosecution Service Inspectorate highlighted the need for a proper deliberation of the persistent offending instead of an assumption that the breach will be prosecuted ahead of substantive offences.\textsuperscript{585} Hence the CPS confirmed in the recently published annual \textit{Violence against Women and Girls} report that one of its future priorities is to refresh the CPS guidance on breaches of restraining orders and the new Stalking Protection Orders.\textsuperscript{586}

Notably, Her Majesty’s Inspectorate Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate joint inspection of Harassment and Stalking Offences found that victims of stalking offences in non-domestic violence cases were less likely to have had a risk assessment.\textsuperscript{587} Crucially the inspectorates made three

\begin{itemize}
\item \textsuperscript{583} Protocol On the Appropriate Handling of Stalking Cases Between the Crown Prosecution Service and ACPO’ (CPS, 2014) <www.cps.gov/publications/agencies> accessed 14 August 2014
\item \textsuperscript{584} Christopher Benitez, Dale McNiel and Renée Binder ‘Do Protection Orders Protect?’ (2010)
\item \textsuperscript{585} 38 Journal of the American Academy of Psychiatry and the Law Online September 2010
\item \textsuperscript{587} Annual Violence against Women and Girls report published’ (CPS, 12 September 2019) <www.cps.gov.uk/cps/news/annual-violence-against-women-and-girls-report-published-0> accessed 12 September 2019
\end{itemize}
significant observations; i) firstly, that when risk assessing domestic abuse victims, the specific questions relating to harassment and stalking were sometimes overlooked. ii) Some victims of harassment and stalking are left unprotected because the risks to them are not assessed routinely. iii) Lack of risk assessment adds to the problems of victims who believe that they are not taken seriously. It is important to note that the third observation echoes the findings of this thesis that cyberstalking is not routinely regarded as a serious offence.

Following publication of the findings, the CPS introduced a new joint protocol which replaced the previous agreement that was introduced in 2014 by the CPS and the Association of Chief Police Officers. The new joint protocol highlights that the police are required to ensure that the Domestic Abuse, Stalking and Honour Based Violence risk assessment (DASH) or other appropriate risk identification or screening tool (including SASH) are used for two purposes. The first purpose is to assess the risk to the victim. The second purpose is to identify safety measures and manage the risk to victims of harassment and stalking.

The participants also expressed frustration at the inability to assess and manage the risk posed by anonymous cyberstalkers who use fake internet accounts to harass victims because their identities are unknown (PRO12 and PO13 and PO21: Chapter 4, page 255) The participants stated that this situation has enabled anonymous cyberstalkers to be one step ahead of law enforcement officers who cannot risk assess and manage the threat they pose to victims (PRO7: Chapter 4, pages 274 and 275).

---

588 ibid
Kropp, Hart and Lyon emphasise that violence risk assessment entails two aspects. The first aspect is the evaluation of individuals to identify the risk as to whether they will perpetrate acts of violence. The second aspect of risk assessment is to develop interventions to manage or reduce that risk. Therefore, Kropp, Hart and Lyon argue that professionals should ascertain the factors that are present in a case that might enhance or increase risks and also assert that the risk assessment of stalkers is simple because victims of any future violence are obvious. From a critical perspective, given that cyberstalking is an aspect of stalking which enables offenders to escalate their harassment of victims from the cyber realm to the physical realm, the researcher argues that legal professionals will be unable to risk assess anonymous cyberstalkers whose risk to victims cannot be assessed, monitored and managed.

The current research findings identified that officers and prosecutors acknowledge that some cyberstalkers are mentally ill and require treatment. Therefore, from a rehabilitative perspective, Mackenzie and James stress that the treatment of stalkers is crucial to resolving the problems motivating stalkers to offend and acknowledge that civil law remedies such as restraining orders may be ineffective.\textsuperscript{591} Mackenzie and James also emphasize that implementing a framework for establishing the factors and determining the delivery of service is important. The researcher argues that Mackenzie and James’ observations are only applicable to cases involving offenders whose identities are known given that some cyberstalkers are anonymous.\textsuperscript{592} The difficulty in such cases is that criminal and mental health professionals will be unable to develop

\textsuperscript{591} Rachael Mackenzie and David James ‘Management and Treatment of Stalkers: Problems, Options and Solutions’ (2011) 29 Behavioural Sciences and The Law 2
\textsuperscript{592} Ibid
a framework that is created to treat the anonymous offender, identifying risk factors and shape the delivery of treatment.

The above observations reveal that the anonymity of cyberstalkers, cyberstalking victims in domestic violence cases having intermittent relationships with offenders, cyberstalkers breaching restraining orders and the inability to risk assess mentally ill cyberstalkers are issues which hinder police officers and prosecutors in the risk assessment of victims and offenders. The findings also reveal that in some cases, restraining orders do not deter offenders from committing further offences against victims after risk assessments have been completed by police officers. From a risk assessment perspective, the implications are that this may result in offenders persisting in the victimization of individuals and jeopardizing the safety of victims by engaging in criminal behaviours which could lead to the materialization of identified risks. From a victimization perspective, another complication of cyberstalkers breaching restraining orders is that it will result in victims fearing for their safety due to the unpredictable nature of cyberstalkers who sometimes, escalate stalking in the cyber realm to stalking in the physical realm.

5.3.5 Evidential difficulties

‘Evidential difficulties’ was the sixth main theme identified in the study. Once again the researcher was aware that the issue of bias could lead to the participants fearing repercussions from their employers. Consequently, to avoid bias the researcher implemented the strategy of seeking clarifications in a sensitive manner and not being
judgmental. These measures put the participants at ease and enabled them to feel free to express their views.

A majority of the prosecutors shared the perception that various perceived evidential difficulties hinder them during the investigation and prosecution of cyberstalkers. Given that prosecutors require digital evidence to build robust cases against cyberstalkers, the participants shared the frustration that anonymous cyberstalkers cannot be successfully prosecuted due to lack of evidence to satisfy the evidential burden of proof as previously discussed earlier in the thesis (Chapter 2, section 2.3.8). The participants stressed that an inability to obtain charging decisions from the CPS is challenging for police officers because they cannot provide the evidence required to prosecute suspects (PO10, PO14 and PO19: Chapter 4, pages 265 and 266). The participants also acknowledged that there is a high evidential threshold to be met given that the CPS will not prosecute a case unless there is a realistic prospect of conviction. From a technological perspective, Reyns highlights that cyberstalkers have various tools at their disposal to enable them to engage in their deviant behaviour which includes desktop computers, laptops, mobile phones, and portable Wi-Fi devices. Hence, Vallcampa and Salat emphasise that prosecution of cyberstalking offences is dependent on forensic analysis of devices capable of communication with a victim.

---

593 The significance of meeting the evidential threshold as previously discussed in paragraphs 2.3.7 and 2.3.8 respectively, is that the CPS will not prosecute suspects if the police do not provide credible, reliable, supporting and strong evidence that is required to build strong cases against the cyberstalkers.
595 Graeme Horsman and Lynne Conniss ‘An Investigation of Anonymous and Spoof SMS resources used for the purpose of cyberstalking’ (2015) 13 Digital Investigation
The participants discussed the challenges that they face in identifying anonymous cyberstalkers which hinder the investigation process. The issue of anonymous electronic communication by cyberstalkers poses investigative difficulties for police officers as are prevent them from obtaining the digital evidence that is required to prosecute cyberstalkers.\textsuperscript{596} Hence, Amichai-Hamburger notes that anonymity on the internet enables an internet user to communicate online without disclosing information.\textsuperscript{597} From the perspective of preserving evidence, Sammon indicates that a preservation order will prevent an ISP from deleting existing data pertaining to an internet subscriber that arguably includes a cyberstalker.\textsuperscript{598} However, a participant expressed the view that it might be a challenge for UK police officers to obtain the required preservation order if a cyberstalker is anonymous.

From a legal perspective, the perceived evidential difficulties highlighted above, hinder prosecutors from building strong cases and meeting the evidential and public interest tests as defined by the CPS code for crown prosecutors. Crucially as previously discussed, (Chapter 1, section 1.2.4), based on the evidential test, UK prosecutors will have to decide whether the evidence presented is sufficient and credible to charge a cyberstalker and whether there is a realistic prospect of convicting him. Additionally, if there is sufficient evidence to warrant a prosecution or settlement out of court, prosecutors will also be required to apply the public interest test to decide whether it is indeed in the public interest to prosecute a cyberstalker?\textsuperscript{599}

The relationship of these various issues to evidential difficulty are illustrated in figure 5.3.5.

\textsuperscript{596} The issue of anonymous cyberstalkers may impede the efforts of police officers to gather the evidence required to tackle cyberstalking as an aspect of cybercrime and prosecute cyberstalkers
\textsuperscript{597} Yair Amichai-Hamburger ‘The Social Net understanding Our Online Behaviour’ (2\textsuperscript{nd} edn, OUP 2013)
\textsuperscript{598} John Sammons, ‘ Digital Forensics: Threatscape and Best Practices’ (first edn, Syngress, 2015) 62
\textsuperscript{599} ibid
Figure 5.3.5. Issues that lead to evidential difficulties identified by participants.

From an evidential perspective, Geach and Haralambous suggests that further investigative difficulties for police officers are establishing the computer that was used by a cyberstalker to disseminate offensive messages and proving the identity of the cyberstalker given that the relevant computer may have been located in a public library.
or internet cafe. A minority of the participants highlighted this issue in relation to cyberstalkers who live in a shared accommodation property and who may argue that a third party used their computer without their consent to harass victims (PO21:Chapter 4, page 271).

From a privacy perspective, Koops and his colleagues argue that the right to privacy as guaranteed under Article 8 of the European Convention of Human Rights 1953, governs the processing of data relating to the private life of individuals which implicitly includes the likes of cyberstalkers and other criminals. Given that cyberstalkers can argue that they have a reasonable expectation of privacy in relation to the information stored on their electronic devices which should not be subject to police investigations, there is a further onus on UK police officers to ensure that there is a legal basis for obtaining publicly accessible data on the internet which pertain to cyberstalkers.

While discussing the legal requirements for establishing offences under the PHA, the participants explained that the prosecutors may not be in a position to meet the legal requirement under s4A of the PHA if it cannot be proven that the actions of an anonymous cyberstalker caused a fear of violence because the identity of the offender is unknown. The participants therefore emphasised that the legal issue is proving that the actions of an anonymous cyberstalker created a fear of violence given that a high evidential threshold has to be met by prosecutors seeking to charge an offender under a section 4A of the PHA.

600 Neal Geach and Nicola Haralambous, ‘Regulating Online Harassment: Is the Law Fit for the Social Networking Age?’ (2009) 73 (3) 73 Journal of Criminal Law 3
602 ibid
603 This legislative provision criminalizes the offence of stalking involving the fear of violence as previously discussed in paragraph 2.3.5.
While discussing the evidential threshold for proving the offence of fear of violence, the participants explained that if police officers cannot provide strong, reliable and credible evidence to prove that the actions of an anonymous cyberstalker created a fear of violence under s4A of the PHA, it can result in prosecutors charging offenders with lesser offences under sections s2 and 4 of the PHA instead. Hence, Leggett examined the concept of fear of violence under s4A of the PHA based on a judicial reasoning in a fairly recent case. The case is R v Qosja (Robert) which involved a stalker who was charged under s4A of the PHA with the offence of creating fear of violence. In this case, the judge in the court of appeal held that under s4A of the PHA, it was for the jury to consider not only whether the complainant feared imminent violence, but also whether she feared that violence would take place in the future.

Likewise, Gowland argues that several grave stalking cases that fall barely short of s.4 of the PHA are charged instead under s.2 of the PHA due to the difficult requirement that the victim fears violence will be used. Importantly, Golwand highlights that there is a huge sentencing gap between the two offences (see Chapter 2, sections 2.3.3 and 2.3.4). Therefore, Gowland suggests that the sentencing powers on s. 2 conviction should either be increased or the offence made a triable offence either way as proposed by the parliamentary inquiry, to ensure that serious s. 2 cases are adequately sentenced. Gowland’s view echoes the frustration of the participants in this research who explained that a legal challenge for prosecutors is proving that a victim was in fear of violence under s4A of the PHA because there is a higher evidential

---

605 [2016] EWCA Crim 1543
607 ibid
burden on the prosecution to prove that the actions of a cyberstalker had a substantial adverse effect on the day to day activities of a victim.

While discussing cases which are discontinued by the CPS due to lack of evidence, the participants stressed that in domestic violence cases, it is difficult to obtain evidence from victims especially if certain victims still want to maintain a relationship with their cyberstalkers. Importantly, the participants revealed that the bigger concern for them was that victims will lose faith in the criminal justice system if they report cases to the police and are subsequently told by police officers that their cases have been discontinued due to insufficient evidence. Therefore, the participants stated that the legal issue of cases not meeting the evidential threshold, could stop some victims from reporting case. The participants explained that this issue is concerning because in some domestic violence cases, cyberstalking can lead to fatalities. Thus, Mackintosh and Swann highlight that the number of individuals killed due to domestic violence in the UK is at its highest level in five years\textsuperscript{608}

Additionally, the participants also shared the perception that other difficulties include the reluctance of domestic violence victims to support the prosecution of cyberstalkers (PRO14 and PRO17, Chapter 4, page 283). Consequently, Vilhaeuer highlights that domestic violence cases are often characterized by the evidentiary issue of victims refusing to support prosecutions.\textsuperscript{609} Notably, Vilhaeuer emphasises that the nature of domestic violence creates an entangled relationship between victim and perpetrator that is not encountered in most other crimes.

\textsuperscript{608} Thomas Mackintosh and Stephen Swann ‘Domestic Violence Killings Reach a Five Year -High’ (BBC, 13 September 2019) <https://www.bbc.co.uk/news/uk-49459674> accessed 26 December 2019

The abuse of technology in domestic violence and stalking cases was investigated by Westbrook based on a survey with 152 domestic violence advocates and 46 victims. The study made three crucial findings.610 The first finding is that stalkers and cyberstalkers implicitly, used technological tools such as phones, tablets, computers, and social networking websites to victimize in intimate partner stalking. The second finding is that perpetrators utilised technology to create a feeling of the omnipresence, and to isolate, punish, and humiliate domestic violence victims. The third finding that was made by Westbrook is that perpetrators also threatened to share sexualized content online to humiliate victims.611

The above findings support the findings of this thesis because it echoes the views of the participants who indicated that some cyberstalkers harass domestic violence victims by hacking into their computers and humiliating them by disseminating obscene sexualized messages in the names of victim. The above findings also confirmed the views of participants who revealed that some victims become isolated and ostracized by their family members after being targeted by cyberstalkers. Additionally, the notion of cyberstalkers punishing victims was echoed by a participant of the researcher's study who revealed that a victim who was constantly punished by an anonymous cyberstalker via numerous silent calls at all hours of the day was mentally and psychologically traumatised which left suicidal and dependant on anti-depressants after seeking medical help.

---

610 Delanie Woodlock 'The Abuse of Technology in Domestic Violence and Stalking' (2016) 23 Violence Against Women 5
611 ibid
From a statistical perspective, the Crime Survey for England and Wales revealed that in the year ending March 2019, an estimated 2.4 million adults aged 16 to 74 years experienced domestic abuse. This report further revealed that of these, 1.6 million were women and 786,000 were men and that the police recorded 746,219 domestic abuse-related crimes in the year ending March 2019 which is an increase of 24% from the previous year. Although the report did not specify the number of cases that were linked to cyberstalking incidents the findings of the current research reveal that cyberstalking stalking incidents are often linked to domestic violence.\(^\text{612}\)

It is important to note that the issue of the lack of victim disclosure of evidence in criminal cases was recently addressed by the CPS in relation to the handling of mobile phone data in rape cases.\(^\text{613}\) The CPS recently emphasized that mobile phone data, or social media activity, will only be considered by the police when crucial to a specific case. Importantly, the CPS indicated that this requirement is necessary to ensure that investigations are fair for both complainant and suspect, all reasonable lines of enquiry must be pursued. The researcher is of the view that this process is currently being applied by police officers in the investigation of cyberstalkers because they are required to obtain, retrieve and analyse offensive electronic messages that have been disseminated by cyberstalkers which constitute electronic evidence and are crucial to cases. The researcher anticipates that this process will enable the CPS to build robust cases against given that only credible evidence that are crucial to the prosecution of


offenders will be considered by police officers and prosecutors during the investigation
prosecution processes respectively.

From a legal perspective, the perceived evidential difficulties highlighted above, hinder
prosecutors from building strong cases and meeting the evidential and public interest
tests as defined by the CPS code for crown prosecutors. Crucially, based on the
evidential test, UK prosecutors will have to decide whether the evidence presented is
sufficient and credible to charge a cyberstalker and whether there is a realistic
prospect of convicting them (see Chapter 1, section 1.2.4). Additionally, if there is
sufficient evidence to warrant a prosecution or settlement out of court, prosecutors will
also be required to apply the public interest test to decide whether it is in the public
interest to prosecute a cyberstalker.614

In summary, the research findings discussed in relation to existing literature
demonstrate that there are various aspects of evidential difficulties that hinder UK
police officers in the prosecution of cyberstalkers. The findings reveal that participants
were exasperated by the perceived evidential problems because they felt that the
problems enabled anonymous cyberstalkers to be a step ahead of police officers given
that cyberstalkers cannot be prosecuted unless they are identified, arrested,
questioned and charged after being evidentially connected to offences.

5.3.6. Victim Behaviour

614 ibid
'Victim Behaviour' was the seventh theme identified in the study. While discussing victim behaviour, participants stated that cases are sometimes not prosecuted due to underreporting of incidents by victims. The participants shared the perception that victims do not report incidents for a variety of reasons. Some of these reasons are; the perception that cyberstalking incidents are trivial, victims will be wasting the time of police officers by reporting incidents, cyberstalkers will not be successfully prosecuted even if victims testify, victims lack faith in the criminal justice system and fear of repercussions from the cyberstalker and his family. This finding resonates with that of Vallacampa and Salat’s research as to the reasons why stalking and cyberstalking victims implicitly, do not report incidents and the use of protection systems by stalking victims. Vallacampa and Salat found that victims rarely report stalking and cyberstalking cases implicitly, due to a lack of confidence in the criminal justice system. Their research revealed that victims gave six reasons why they did not report incidents; lack of evidence, fear of repercussion, unwillingness to punish the criminal, the belief that it was a private matter or that it was not serious enough to justify reporting, and a lack of confidence in the effectiveness of the criminal justice system and fear of secondary victimisation.

Likewise, Al-khateeb, Epiphaniou, Alhaboby and others, investigated the role of Police, Mobile Operators, Internet Service Providers, and owners/administrators of online platforms regarding intervention in response to offences. The study was based on a sample of 305 participants who identified themselves as victims of online...

616 ibid
harassment. Notably, in relation to the reporting of incidents, the study made three important findings. The first finding is that some of the victims did not notify the police of incidents due to various reasons which include fear of escalation, feelings of guilt, sympathy and self-blaming. The second finding is that an outstanding number of victims did not report incidents to their service provider because they were not aware that they could. The third reason is that the victims who had reported incidents to the ISPs revealed that either no or very little support was offered. The first findings of Al-khateeb, Epiphaniou, Alhaboby and others echo the views of the participants in the researcher’s study who explained that sometimes, victims of cyberstalking do not report offences to the police for various reasons. The reasons are that they feel that the offence is trivial, they will be wasting the time of police officers by reporting incidents and that cyberstalkers will not be successfully prosecuted even if victims testify against them in court.

The researcher’s findings and the findings of Al-khateeb, Epiphaniou, Alhaboby and others, attribute the issue of victims not reporting cyberstalking incidents to the police to a variety of reasons. Al-khateeb, Epiphaniou, Alhaboby and others found that victims had various personal reasons for not reporting incidents to the police. Likewise, the researcher’s study found that victims do not report cyberstalking incidents to the police for various reasons which are linked to a lack of confidence in the criminal justice system.

Participants in the current research also expressed frustration at victims who refuse to testify in court and thereby hindering prosecutors from building strong cases against offenders (PO13: Chapter 4, page 286). While discussing the reason why some
victims of cyberstalkers refuse to attend court, the participants explained that the reason for this issue is because some victims fear repercussion from the cyberstalker and his family. This issue was once again highlighted by Vallacampa and Salat.618

Figure 5.3.6. Illustrates the types of victim behaviour that participants perceive hinder the successful investigation and prosecution of cyberstalkers.

Figure 5.3.6 Victim Behaviour difficulties perceived by participants to hinder the investigation and prosecution process.

---

Participants stated that lack of full disclosure by victims can lead to cases being lost and cyberstalkers not being charged with suitable offences due to victims withholding evidence from the police (PO3, PO17 and PRO29: Chapter 4, pages 284 and 285). The participants emphasised that this aspect of victim behaviour was frustrating because, it provides incomplete pictures of cyberstalking incidents and can lead to the death of victims in some domestic violence cases. Hence Bent-Goodley therefore asserts, from a global perspective, that domestic violence fatality presents obstacles to countries and communities globally.\textsuperscript{619} From a law enforcement perspective, Hill therefore encourages police officers not to ignore reluctant victims in domestic abuse cases but to instead endeavour to build a strong criminal cases against offenders without relying on the victim’s evidence.\textsuperscript{620} Importantly, Hill argues that the actions of a police officer in handling a domestic violence case may prevent an escalation of future acts of violence in the home. From a cybercrime perspective the researcher argues that given that some anonymous cyberstalkers target domestic violence victims, police officers may only be able to prevent an escalation of victimisation emanating from the cyber realm to the physical realm if the identity and location of the is cyberstalker are known.

Likewise, Matos, Grangeia, Ferreira, and others conducted a study on stalking victimization in Portugal and found that nature of the relationship between the victim and the stalker was a primary predictor of stalking ranges and perpetuation.\textsuperscript{621} The study found that the closer the relationship, the greater the diversity and duration and that the stalking impact was higher in victims that experienced more diverse stalking

\textsuperscript{619} Tricia Bent-Goodley ‘Domestic Violence Fatality Reviews and the African Community’ (2013) 17 Criminology and Criminal Justice 4
behaviours and fear. Matos, Grangeia, Ferreira, and others concluded that fear and impact mediate the relationship between stalking diversity and help-seeking. From a domestic violence perspective, given that the study found that the stalking impact was higher in victims that experienced more diverse stalking behaviours and fear, there is an expectation that victims will promptly report stalking and cyberstalking incidents to the police with a view to stopping victimisation and bringing offenders to justice.

It is important to note that the participants indicated that they offer support to victims who are reluctant to testify against cyberstalkers in court (PO17: Chapter 4, page 260). The researcher therefore, acknowledges that under the Youth Justice and Criminal Evidence Act 1999, the CPS can offer vulnerable and intimidated witnesses various measures that can assist them in giving evidence in court and to alleviate some of the stress associated with giving evidence.

Although a majority of the participants alluded to the fact that victims of cyberstalkers tend to be females and that offenders tend to be males, the researcher recognises that victims could also, include males and perpetrators females because victimisation and offending are not restricted to a specific gender. The fact that males can be victimised by cyberstalkers is evident in the highly publicized case of Lord McAlpine of West Green v Bercow. In this case, the judges considered the dissemination of electronic communication via Twitter from defamatory and libellous perspectives. In doing so, the judges held that the words will be deemed defamatory if they referred to the claimants and if they had a significant adverse effect on the way people

---

622 ibid
624 [2013] EWHC 1342 (QBD)
approached them.\textsuperscript{625} This case is significant because, it arguably established that the victims of cyberstalking can seek to bring cyberstalkers to justice via civil litigation as opposed to criminal litigation.

In summary, the research findings demonstrate that underreporting, lack of disclosure and reluctant cyberstalking victims in domestic violence cases are perceived aspects of victim behaviour which hinder UK police officers in the prosecution of cyberstalkers. The findings reveal that the participants were hindered by the perceived difficulties associated with victim behaviour because the difficulties lead to cases being discontinued and in some cases to cyberstalkers not being prosecuted. Worryingly, the highlighted aspects of victim behaviour may lead to victims being put at risk particularly in domestic violence cases because the escalation of offending can and has resulted in fatalities.

\textbf{The thesis findings in respect of the research questions:}

This thesis reports on a qualitative study of the perceptions of police officers and prosecutors in London and the factors which frustrate them in the investigation and prosecution of cyberstalkers. Participants shared the perception that several factors impede the investigation and prosecution of cyberstalkers and from the interview data six main themes emerged namely; legislative difficulties, lack of training and knowledge, lack of resources, issues with risk assessment, evidential challenges and victim behaviour. Additionally, the findings have explored and addressed the issue of what might be considered the thresholds of acceptable behaviour on the internet and

\textsuperscript{625} ibid
these thresholds were determined in some part through the participants’ own professional experience. A further objective of the research was to explore the challenges that police officers perceive impede the risk assessment of cyberstalking victims. The findings reveal that participants acknowledge certain factors which hinder the risk assessment of both cyberstalking victims and cyberstalkers particularly where the mental health status of the cyberstalker is in question.

The findings in respect of Research Question 1:

What are the perceptions of police officers and prosecutors on cyberstalking and the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking?

To identify the perceptions of police officers and prosecutors in London on cyberstalking and the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking the results of this research provide a breakdown of several perceptions. The analysis of the qualitative interviews, enabled the researcher to identify the following fifteen perceptions that UK police officers and prosecutors on cyberstalking and the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking; (1) Subjective view of victims (2) Objective view (3) Facts of the case and motive of the offender (4) Impact on victims (5) Gravity of the offence (6) Statutory definition of cyberstalking (7) Intention of the cyberstalker (8) Duration of the conduct (9) Prior relationship with the victim (10) Content of the messages (11) Reaction of the victim, (12) Vulnerability of the victim (13) Request of the victim for the cyberstalker to stop victimization (14) Cyberstalker’s
awareness of the impact of his conduct on the victim Intention of the cyberstalker and
(15) Size of the electronic platform that was used to disseminate messages

In relation to this, Edward discusses behaviours that occur within the parameters of acceptable deviance in relation to deviant acts which are informed by norms and anchored by law. Importantly, Edwards makes a distinction between the regulators and the regulated who can trigger enforcement and social sanctions when behaviours cross the parameters of an acceptable behaviour threshold. The findings of this study reflect the views of Edward given that the participants shared the perception that cyberstalking is a behaviour that does not comply with the law which occurs when various perceived thresholds of the parameters of acceptable behaviour are crossed and therefore, not acceptable to police officers, prosecutors and victims within the law enforcement framework of the regulators and the regulated.

Moreover, Hooper and Kalidas emphasize that various differences between acceptable and unacceptable behaviour online and offline have emerged. Hooper and Kalidas found that stalking or cyberstalking implicitly was identified by the participants as one of nine unacceptable behaviours. Despite the fact, that the research participants are different in age and background, there is a correlation between this study and the study of Hooper and Kalidas because both studies establish that cyberstalking is deemed an unacceptable online behaviour by individuals more especially, from the perspective of the invasion of privacy. Further, both studies highlight that personal beliefs and values guide individuals in determining

---

627 ibid
629 ibid
630 Hooper and Kalias conducted qualitative interviews were conducted with 16 youth, aged 18-20 years, and who had a Facebook account
the behaviours that are unacceptable online and on Social Networking Sites such as Facebook.

**The findings in respect of Research Question 2:**

*What factors do police officers and prosecutors perceive could frustrate them in the investigation and prosecution of cyberstalkers?*

Despite the fact, that the research jurisdictions are different, there is a correlation between this study and the study of D'Ovidio and Doyle.631 This is because the current research findings confirm that there are evidential and legislative difficulties in the investigation of cyberstalkers. D'Ovidio and Doyle highlighted two out of the seven perceived investigative difficulties identified by the participants in the current research. A further comparison can be made between both studies because they suggest that law enforcement officials encounter several difficulties in the investigation of cyberstalkers. Further, both studies highlight the issue of anonymous cyberstalkers as an investigative hurdle and suggest that staff should be trained on how to investigate cyberstalking offences with a view to equipping them with the requisite knowledge and the computer forensic skills required to investigate cyberstalking offences.

From an educational perspective, a crucial comparison can be made between the findings of this thesis and the findings of the independent parliamentary inquiry into

stalking law reform which recommends that the relevant Secretaries of State ensure that criminal justice professionals receive training in anti-stalking legislation as well as on how to identify it.632

The findings in respect of Research Question 3:

What challenges do police officers perceive impede the risk assessment of cyberstalking victims?

To identify the challenges that police officers perceive impede the risk assessment of cyberstalking victims the analysis of the qualitative interviews, enabled the researcher to identify the following 6 challenges which hinder police officers from risk assessing victims;

(1) Anonymous cyberstalkers cannot be risk assessed, monitored or managed

(2) Domestic violence victims who rekindle relationships with cyberstalkers

(3) Lack of knowledge

(4) Shortage of manpower

(5) Cyberstalkers breaching Restraining orders

(6) Victims refusing to implement recommend risk assessment safety measures

In support of this finding, Kropp, Hart and Lyon stress that the risk assessment of stalkers and cyberstalkers implicitly is difficult due to the range of stalking behaviours and lack of research.633 The findings of this thesis therefore, contribute knowledge to this area of research by identifying the above six specific challenges which hinder


police officers in the risk assessment of victims given the fact that cyberstalking consists of a variety of behaviours which have negative impacts on victims.

From a mental health perspective, although Mullen, Mackenzie and James, identify that the risk assessment of stalkers and cyberstalkers implicitly often falls to mental health professionals, this study found that police officers are also tasked with risk assessing victims and managing the risk to victims with a view to countering identified and envisaged threats. Importantly, the findings in relation to this research question identify that the anonymity of cyberstalkers whilst representing a major hindrance to the risk assessment of cyberstalkers by police officers is not the only one.

5.6.4. The Findings in respect of Research Question 4:

Do police officers and prosecutors perceive evidential challenges, victim behaviour, lack of resources, and lack of training as presenting law enforcement difficulties?

In response to this fourth research question, the analysis of the qualitative interviews, enabled the researcher to identify the following significant aspects of evidential challenges, victim behaviour, lack of resources and lack of training which present law enforcement difficulties;

**Evidential Challenges:**

(1) Victims not keeping evidential records  
(2) Cases being discontinued due to lack of evidence  
(3) Police officers not providing further evidence once suspects have been charged  
(4) Prosecutors having to repeatedly chase police officers for outstanding evidence  
(5) Proving an offence under section 4A of the PHA  
(6) Establishing a course of conduct under section 7 of the PHA  
(7) Obtaining evidence from victims in domestic violence cases  
(8) Insufficient evidence to prosecute  
(9) Prosecuting cyberstalkers
who victimize via proxy (10) Domestic violence victims not reporting cases because the evidential threshold cannot be met (11) Anonymous cyberstalkers being one step ahead of police officers (12) Police delays in providing evidence due to heavy caseloads (13) Prosecuting mentally ill cyberstalkers

**Victim Behaviour:**

(1) Victims not supporting prosecutions (2) Victims refusing to testify against cyberstalkers (3) Victims refusing to go through the stress of trials (4) Victims cross communicating with cyberstalkers and giving mixed messages (5) Victims withholding evidence (6) Victims lack of confidence in the police and the criminal justice system (7) Victims fear of repercussions (8) Victims assumption that their cases will be dropped even if they testify (9) Victims not reporting offences (11) Victims delaying in reporting incidents (12) Victims disclosing personal information on the internet (13) Victims continuing relationships with cyberstalkers (14) Victims withholding information on the gravity of offences

**Lack of resources:**

(1) Missed opportunities to risk assess victims and cyberstalkers (2) Shortage of specialist and non-specialist police officers (3) Excessive caseloads (4) An inability to meet CPS deadlines for providing evidence (5) Insufficient time to follow up on initial reports by victims (6) Lack of a centralized database for sharing local intelligence

**Lack of training:**

(1) Tracing IP and email addresses (2) Phone and computer forensic training

These findings are supported by Horsman and Conniss who emphasize that the proliferation of anonymous services make it difficult for digital forensic experts to analyse and detect the origin of stalking and cyberstalking messages implicitly. \footnote{Graeme Horsman and Lynne Conniss ‘An Investigation of Anonymous and Spoof SMS resources used for the purpose of cyberstalking’ (2015) 13 Digital Investigation}

Furthermore, the findings concur with the view of Horsman and Corniss that the prosecution of cyberstalkers is dependent on the availability of the required digital forensic evidence for presentation at court. More importantly, from the subjective perspective of law enforcement officials, the current research goes a step further in establishing that in addition to evidential challenges, police officers perceive victim behaviour, lack of resources and lack of training as constituting investigative and prosecutorial challenges for both police officers and prosecutors.

**Contribution to knowledge:**

In summary, the findings of this thesis therefore, contribute knowledge by highlighting the six specific challenges which hinder police officers in the risk assessment of victims given the fact that cyberstalking consists of a variety of behaviours which have negative impacts on victims. This research also identifies that the risk assessment of mentally ill cyberstalkers is an issue that needs to be addressed by the relevant stakeholders to arguably avoid missed opportunities to both risk assess and develop strategies for countering identified risks to victims and their families. Finally, a major
finding in respect of the risk assessment of cyberstalkers by the police is, that the process is being inhibited by the anonymity cyberstalkers are afforded by the internet. This then implies that police are ultimately impeded from managing the risk cyberstalkers present to their victims which places those victims at constant risk.

5.4 Relation to previous research

Although some of the findings of the research are broadly in line with the views of Van der Aa in terms of establishing that law enforcement officials will encounter evidential, jurisdictional, extradition and legislative difficulties in the investigation and prosecution of cyberstalkers, the research runs counter to Van der Aa’s view regarding the failure of police officers to act. 635 To this effect, the findings are to some extent, at odds with the findings of Van der Aa because the research demonstrates that the police officers interviewed were willing to investigate cyberstalkers but they acknowledged that the investigation of cyberstalkers will be fraught with various perceived investigative difficulties. This appears to indicate that police officers are keen to take an active part in the investigation process by arresting, interviewing and charging cyberstalkers subject to the difficulties revealed in the study being overcome.

Despite the research methods used being different, this research can be compared to the work undertaken by D’Ovidio and Doyle.636 D’Ovidio and Doyle conducted a study on cyberstalking with a view to understanding the investigative hurdles based on the analysis of 201 cases of cyberstalking. D’Ovidio and Doyle examined the outcome of

---

635 Suzanne Van Der Aa, International (cyber) stalking: Impediments to Investigation and Prosecution (Pure, 2011) <www.pure.uvt.nl/ws/files/1310512/Aa_International_cyberstalking_110216_posprint_embargo_1_y.pdf> accessed 9 August 2018
the 201 closed cases with a view to establishing investigative hurdles. Conversely, the current research, utilised interview techniques to obtain research data from 63 law enforcement officials with a view to identifying the difficulties that they encounter in the investigation of cyberstalkers. Both studies share the common factor of researching cyberstalking from a law enforcement perspective and from two important perspectives, the findings are consistent with the previous research of D’Ovidio and Doyle. Specifically, the current findings confirm that there are evidential and legislative difficulties that hinder the investigation of cyberstalkers.

Although previously conducted research has found that police officers may be reluctant to investigate aggravated harassment cases which is arguably synonymous to cyberstalking if the perpetrators and the victims reside in different locations, this study found evidence to the contrary. In effect, this study found that although the police officers who were interviewed for the study were willing to investigate cyberstalkers, they were nevertheless frustrated by the fact that the six perceived law enforcement difficulties which have been highlighted in Chapters 4 and 5 respectively will hinder police officers in the investigation and prosecution of cyberstalkers.

In addition, the findings of this research are to some extent, opposed to those of DreBing and his colleagues who conducted an online survey of 6,379 participants on the prevalence of cyberstalking. The research findings of DreBing and his colleagues revealed that most cases involved former partners and concluded that legal authorities should take cyberstalking seriously given that the negative impact of

---

637 ibid
638 ibid
cyberstalking is similar to online stalking. The findings of the current research run slightly counter to the view of DreBing and his colleagues given that it found that domestic violence cases were not the highest category of cyberstalking cases that London police officers investigated but was the second highest category of cases that had been prosecuted. In contrast, the research found that the cyberstalking of strangers was the highest category of cases investigated by UK police officers. It should be noted that the research of DreBing and his colleagues were confined to the German jurisdiction and comprised of a large population sample that consisted of members of the public. Whereas in comparison this study was confined to the UK jurisdiction and consisted of a much smaller population sample comprising of law enforcement officials.

From a legislative perspective, the findings of this study concur with the views of Hazlewood and Koon-Magnin, who examined the legislation on cyberstalking and cyber harassment within the 50 states of the US with a view to establishing a clear definition for cyberstalking and cyber harassment. Their findings too suggest that the investigation of cyberstalking and cyber harassment is synonymous with a lot of challenges ranging from the anonymity of cyberstalkers to jurisdictional issues.640

Furthermore, the findings of this research, reflect the recent views of the Crown Prosecution Service Inspectorate and Her Majesty’s Inspectorate of Constabulary following publication of their report findings on 5 July 2017 concerning how the police and the CPS tackle stalking and harassment. The report found that there is no single,

consistent definition for stalking.\textsuperscript{641} However, the findings of this thesis are to some extent, at odds with the conclusion of the inspectorate because it reveals that the police officers and prosecutors interviewed for the study are keen to prosecute cyberstalkers but acknowledged that they will encounter several difficulties during the investigation of cyberstalkers. The Crown Prosecution Service Inspectorate and Her Majesty’s Inspectorate of Constabulary inspected 112 cases of stalking and harassment and established that the cases had not been dealt with effectively. It is important to note that the findings of this research were identified prior to the publication of the inspectorates’ report.

5.5 Theoretical implications

The qualitative research method was applied to the study. This method afforded the researcher the opportunity to conduct the research and to gain an insight of the cyberstalking phenomenon from the subjective perspective of the participants.\textsuperscript{642} In doing so, the researcher applied the epistemological assumption which postulates that the most effective way to understand a phenomenon is to recognize that there is no single unitary reality apart from our perceptions given that each individual has a point of view and experiences a different reality.\textsuperscript{643} This approach enabled the researcher to analyse the various subjective views of the 63 law enforcement officials.


\textsuperscript{642} Evelyn Jacobs, ‘Clarifying Qualitative Research: A Focus on Tradition’ (1988) 17 (1) Educational Researcher, 16

The qualitative research method was effective because it allowed for the exploration of the participant’s views on the phenomenon of cyberstalking from a law enforcement perspective. A dual approach was adopted towards the analysis of data. The first phase entailed the researcher transcribing the interview transcripts and analysing the data segment by segment with a view to highlighting the key words in text. The first phase was the basis for the preliminary analysis of data and also entailed the breaking down and coding of data to confirm the key words in the textual data. This phase highlighted seventeen themes as the data was voluminous. The second phase of the research entailed categorizing the seventeen themes into seven main themes. This dual approach to data analysis was significant because it ensured that the data was analysed in detail.

In addition to an analytical lens, the findings were considered from a theoretical lens. Hence, the deterrent theory was applied to the findings. From a historical perspective, the deterrence theory can be attributed to Jeremy Bentham and Cesare Beccaria. Notably, Jeremy Bentham postulated that offences occurred from the conscious, rational considerations of the individual. According to Jeremy Bentham, a person contemplating the commission of a crime would undertake a cost-benefit analysis and would engage in a criminal activity only if potential benefits sufficiently outweighed expected costs. From a law enforcement perspective applying this line of reasoning to cyberstalkers who breach restraining orders in particular, it is arguable that such cyberstalkers continue to offend because after applying a cost-benefit analysis, they

\[\text{ibid}\]
believe that the gain of committing cyberstalking offences outweighs the risks or costs of committing such activities.  

From a mental health perspective applying Bentham’s theory in this era of mental health awareness, it is arguable that there is a growing recognition that not all offenders have decided to commit offences after weighing up the benefits and costs of committing criminal acts given that some of them are mentally unwell. Worryingly, O’Keefe asserts that the police and the public still have negative attitudes towards offenders with mental health problems. Furthermore, O’Keefe argues that the awareness campaigns and additional training, which have previously been successful at reducing negative attitudes are probably not as effective as previously assumed. Angermeyer and Dietrich investigated public attitudes and beliefs towards people with mentally illness. From a positive perspective, Angermeyer and Dietrich argue that due to an increase in knowledge and awareness, the negative attitude towards mental health issues is decreasing. Likewise, Savrun, Arika, Usyal and others emphasize that factors such as personal experience, education, occupation or being female can result in a reduction in the negative stigmatisation towards the mentally ill. To this effect, the current campaign to increase awareness on mental health albeit in respect of the treatment of mentally ill stalkers and cyberstalkers implicitly is evidenced by the creation of the National Stalking Clinic in 2011 for the treatment and rehabilitation of offenders as previously discussed in Chapter 2, section 2.7.

---

645 It could be argued that the convicted cyberstalkers who breach restraining orders are not deterred by the imposition of restraining orders as a punishment.  
648 Angermeyer and Dietrich emphasise that the there is a perception that mentally ill individuals are unpredictable and dangerous which is attributable to the reasons why people fear the mentally ill  
649 Bayram Savru, Mert Arikan, Kemal Usyal, Omer Cetin, Borc Poyraz, and others ‘Gender Effects on Attitudes Towards the Mentally ill: A Survey of Turkish University Students (2007) 44 Israel Journal of Psychiatry and Related Sciences 1
From a general perspective, applying the deterrence theory to explain cyberstalking, it might be argued that cyberstalkers are rational economic actors who engage in criminal activities after applying a cost-benefit analysis prior to offending. From a legal perspective, the challenge therefore for law makers is to enact laws which will make criminals decide that the risks, or costs, of engaging in cyberstalking activities is so great that it outweighs the gain from committing such a crime.

Kennedy stresses that that the deterrence theory promotes communicating the deliberate threat of harm to the public in a bid to discourage socially proscribed conduct across societies. The researcher argues that some cyberstalkers as members of the public may not be deterred especially if they are anonymous. From a punitive perspective, Kennedy further highlights that punishment, as a means for conveying the deterrence message, creates inhibitions against committing crimes which are conscious and unconscious and results in continued societal compliance.

It is questionable whether this line of reasoning can be applied to cyberstalking as a cyberenabled crime given that the internet enables offenders to communicate anonymously and via the use of pseudonyms or fake details in a bid to avoid detection. Additionally, cyberstalkers can buy mobile phones for targeting victims which not require a registered name as a means of avoiding detection, investigation and prosecution. This is issue was highlighted by a participant who explained that he had been unable to prosecute some cases anonymous cyberstakers who victimized individuals via the use of unregistered SIM cards and pay as you go mobile phones.

651 ibid
because their identities could not be unmasked. Therefore, Hazelwood and Koon-Magnin highlight that it makes additionally difficult to identify and track offenders, and can further worsen the fear and apprehension felt by the victim, who may not know who is harassing, stalking or cyberstalking him or her implicitly.652

From a different punitive perspective, Smith and Bailey emphasise that severity and certainty of punishment are two additive factors which are suggested by the deterrence theory.653 Crucially, Smith and Bailey assert that when punishments are severe and administered with certainty, maximum deterrence results. The findings of this study demonstrate that a minority of the participants were frustrated at the perceived leniency of sentencing which some cyberstalkers received. Hence applying Smith and Baileys’s reasoning, it can be argued that some cyberstalkers may continue to offend if the punishment that they receive is not severe enough to deter them from future continuous offending.

Draper emphasizes that Jeremy Bentham’s theory of punishment postulates that sentences should be proportionate to the crime committed.654 Similarly, Tomlinson notes that the classical deterrence theory posits that punishments should be swift, certain, and proportionate to the crime in order to effectively deter individuals from committing crimes.655 Given that the findings of the study reveal that the participants shared frustration at the lenient sentencing dealt to cyberstalkers it could be argued that such participants were frustrated because, they were of the view that the

---

sentences given to some cyberstalkers were not proportionate to the offences committed. However, in the current research the participants did not highlight delays and uncertainty of punishments as issues which frustrate them in the investigation of cyberstalkers.

Further Tomlinson in highlighting the basic principles of classical theory, acknowledged that Cesare Beccaria advocated for laws that were clearly written and for enlightening the public on the law and its applicable punishments to educate people about the consequences of their behaviour. The findings of this thesis reveal that the participants shared the perception that cyberstalkers still offended especially in domestic violence cases despite the criminalization of stalking and cyberstalking implicitly by the amended PHA.

In light of the above observations, there are two theoretical assumptions based on the deterrent tenet on how punishment may deter cyberstalkers. The first assumption is that the certainty of punishments and increasing the likelihood of punishment may deter people from engaging in criminal conducts. The second theoretical assumption is that the severity of punishment for a particular crime may influence a behaviors if a potential offender concludes that the punishment is so severe, that it is not worth the risk of getting caught. Hence, Mungan, explores whether the certainty of punishment is a more severe deterrent than the severity of punishment.

The findings further revealed that the participants expressed frustration at anonymous cyberstalkers who cannot be prosecuted or issued harassment warning notices.

---

656 ibid
657 Murat Mungan ‘Salience and the severity versus the certainty of punishment’ (2019) 57 International Review of Law and Economics
because their identities are unknown. The finding additionally revealed that some police officers lack the knowledge required to unveil the identities of anonymous cyberstalkers. From a punitive perspective, it can therefore be argued that even if the punishment in the UK for committing cyberstalking are swift and severe, the measures would not deter anonymous cyberstalkers who continue to offend because some of the law enforcement officials lack the specialist knowledge that is required to unveil the identities of the offenders.

The findings further highlighted that the participants expressed frustration at cyberstalkers who continue to offend after they have been convicted by breaching restraining orders. This finding therefore demonstrates that cyberstalkers who breach restraining orders are not deterred by the threat of punishment hence their decision to continue to victimise individuals. Given that the participants expressed frustration that some victims do not report offences because they lack confidence in the criminal justice system, it is arguable that the threat of certain and swift punishments for engaging in cyberstalking offences may not deter certain cyberstalkers if they know that victims will not report the offences especially if the cyberstalkers are anonymous. This is more so because, a participant highlighted a case which involved a cyberstalker who breached the terms of a restraining order by contacting a victim and subsequently murdering her. The case therefore demonstrated that the punishments imposed on certain criminals such as cyberstalkers, may not deter them from committing further offences if the offenders are determined to persistently victimise individuals regardless of the threat of punitive sanctions.

---

658 The participants were frustrated because they were of the view that cyberstalkers who persistently offend, waste the time of criminal justice officials who have and prolongs the ordeal of victims.
From a technological perspective, the internet enables cyberstalkers to communicate instantaneously, anonymously, cheaply and globally. Therefore, in light of the above research findings with regards to cyberstalkers breaching restraining orders, victimisation by anonymous cyberstalkers and underreporting by victims, it is questionable from a theoretical perspective whether the deterrence theory can be applied to cyberstalking as an aspect of cybercrime. Hence, Taddeo acknowledges that the success of cyber deterrence is greatly reduced by factors such as anonymity, global reach and the inter-connectedness of information networks.\(^{659}\) Notably, Taddeo argues that these factors can render the success of cyber deterrence entirely ineffective.

From a law enforcement perspective, it may be difficult to police cyberstalking as a cyber-enabled crime because it is a transnational crime. Hence, Brenner and Scherwta emphasise that the fact that cybercrime transcends national boundaries causes investigative issues because the procedural laws that govern the conduct of criminal investigations only apply to the countries which enacted the laws.\(^{660}\) Therefore, Brenner and Scherwta examine the legal issues emanating from the use of computers ranging from legislative to evidential issues.\(^{661}\)

From an international perspective, Jingiong highlights that the current system of cooperation between countries is inefficient for dealing with international issues arising from cybercrime given that the electronic evidence of cybercrime can be easily

---


\(^{661}\) ibid
damaged and therefore, requires countries to promptly obtain evidence. Applying Jingiong’s reasoning to the cyberstalking as an aspect of cybercrime, it is arguable that UK police officers will encounter the international issues highlighted by Jingiong in the investigation of cybercrime more especially, given its transnational nature. Therefore, Grabosky emphasizes that transnational cybercrime will always be a challenge partly due to the borderless nature of cyberspace particularly in relation to organized criminal groupings.

Given the above, Strancu and Andrei stress that cybercrime is a grave issue which requires a strong technical and legal response. Strancu and Andrei therefore highlight that cyber criminals are permanently developing new and ingenious methods to hack into systems. Given that cyberstalking is a cyber-enabled aspect of cybercrime Strancu and Andrei’s line of reasoning can be applied to cyberstalkers who sometimes, hack into the computers of victims.

5.6 Summary of the research

The ability of UK police officers and prosecutors to bring cyberstalkers to justice is contingent on whether they can successfully prosecute the perpetrators given that cyberstalking is an anonymous behaviour which is perpetrated in the virtual world.

The researcher has provided the findings from the two perspectives of i) identifying the perceptions of police officers and prosecutors in London of the factors which

---


663 Peter Grabosky ‘The Borderless Dimension of Cybercrime’ 6 GC 1

664 Victoria Stanciou and Andrei Tinca ‘Exploring cybercrime – realities and challenges’ 2017 16 AMIS 4
frustrate them in the investigation prosecution of cyberstalkers and ii) establishing what could be considered the threshold of acceptable behaviour on the internet. The findings reveal that participants shared the perception that six factors impede the investigation and prosecution of cyberstalkers. The findings further reveal that the participants identified various thresholds of acceptable behaviour viewed through the lens of their own professional experience.

Therefore, the four pronged, objectives of the thesis are important because;
1 The objectives identify the perceptions of police officers and prosecutors on cyberstalking and the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking.
2 The objectives examine the factors which police officers and prosecutors perceive could frustrate them in the investigation and prosecution of cyberstalkers.
3 The objectives explore the challenges that police officers perceive impede the risk assessment of cyberstalking victims.
4 The objectives investigate whether police officers and prosecutors perceive evidential challenges, lack of resources and lack of training as presenting law enforcement difficulties.

5.7. Strengths and limitations of the research

5.7.1 strengths

*Extensive information reinforcing credibility of the data*
The seven themes of investigative difficulties were established via a breakdown of the primary data obtained from the interview transcripts (n=55) of the police officers and prosecutors. Additional data was obtained from the four transcripts of UK law enforcement officials. The large amount of data collected ensured that the data was credible and this was reinforced when theoretical saturation was reached during the interview process.

**Recruitment of prominent law enforcement officials**

The research involved participants who were top ranking law enforcement officials. Two of the four additional senior UK participant law enforcement officials were involved in the criminalisation of cyberstalking at the time of the study. The first senior law enforcement official was a prominent member of parliament who was appointed by the coalition government to chair the independent parliamentary inquiry on stalking. The participant was able to provide views based on first-hand experience from legislative, investigatory and governmental perspectives.

The second senior law enforcement official is an Assistant Chief Constable and the Association of Chief Police Officers Lead on stalking and harassment in the UK. Due to the prominent nature of his job, the participant was able to provide detailed data based on his experience in investigating cyberstalkers.

The third prominent law enforcement official who was interviewed is the former chief executive of the national probation service who was a part of the independent
parliamentary inquiry on stalking. The participant provided data from the perspective of a probation official.

The fourth UK law enforcement official recruited is a senior policy advisor for the Northern Ireland government who assists the Northern Ireland government in drafting laws. The participant contributed to the study from the perspective of a government official who assists in the drafting of government policies. The participant was responsible for assisting the ministry of justice legislatively by conducting researches and reporting back to governmental officials on proposed legislative changes. The participant confirmed that in Northern Ireland, at the time of the study the current legislation on harassment was still being used to prosecute stalkers and cyberstalkers because there was no specific legislation on either stalking or cyberstalking in Northern Ireland. The participant further indicated that although some London representatives of stalking charities had lobbied the Northern Ireland government for legislative changes, at the time of the study, the public prosecution service in Northern Ireland was content with the current law on harassment as a tool for the prosecution of cyberstalkers.

In addition to the above, the researcher interviewed three senior borough crown prosecutors who provided significant data from a prosecutorial perspective. The findings of the study highlight that the police officers and the prosecutors share common views regarding the difficulties that law enforcement officials face in the investigation of cyberstalkers and the law enforcement methods of international cooperation.
Diverse sample based at different work locations

As previously mentioned, the participants consisted of 25 police officers, 30 prosecutors and 4 UK law enforcement officials. The participants were based in different London office locations and had varied law enforcement backgrounds. Consequently, they were able to answer the research questions from various professional viewpoints which reflected their different experiences, and this enriched the data gathered.

5.7.2 Limitations

The study is significant because it investigates the perceptions of police officers and prosecutors in London of the factors which frustrate them in the investigation and prosecution of cyberstalkers and the threshold of acceptable behaviour on the internet. Nevertheless, it has four limitations;

Research Bias

Given that the researcher has been employed by the CPS for over fifteen years, the researcher was aware that her professional background could lead to bias and prevent the participants from fully discussing the factors which frustrate them in the investigation and prosecution of cyberstalkers. Therefore, bias was a limitation of the study. As previously discussed in Chapter 3, section 3.1 bias is present in all research
and is difficult to eliminate.\textsuperscript{665} Hence, Barusch, Gringeri and George emphasise that some researchers have conducted their studies to minimize bias given the pervasive effects of human limitations and subjectivity which may impede the potential objectivity of social work research.\textsuperscript{666} Consequently, to address the limitations of the study regarding bias with a view to conducting a rigorous study, the researcher implemented several measures. This more so because, Mark and Poon stress that existing sampling methods can produce biased outputs and stress that existing sampling methods require modifications to alleviate the bias.\textsuperscript{667} Additionally, Mackieson, Shionsky and Connolly acknowledge that there are criticisms of bias regarding the lack of rigour in qualitative research that is conducted by social researchers.\textsuperscript{668} Therefore, they highlight that academics have indicated that in reality, bias may occur because of varied value assumptions in the conduct of any method of research.\textsuperscript{669}

The research bias issues that were discussed in paragraph 3.1.1 did not arise because the researcher developed a professional rapport with the participants who felt comfortable in her presence and were therefore willing to discuss the perceived difficulties that they encounter.

As previously discussed in detail in Chapter 3, (section 3.2), the researcher adopted several measures in a bid to eliminate bias. The measures ranged from recruiting

\textsuperscript{665} Joanna Smith and Hele Noble ‘Bias in research’ (BMI, 2014)
\textsuperscript{665} Anna Maria Simundic ‘Bias in research’ (2013) Biochem Med (Zagreb) 23 (1)
\textsuperscript{666} Amanda Barusch, Christina Gringeri and Molly George (2011) ‘Rigor in qualitative social work research: A review of strategies used in published articles’
\textsuperscript{668} Penny Mackieson, Aron Shionsky and Marie Connolly ‘Increasing the Rigour and Reducing Bias in Qualitative Research: A Document Analysis of Parliamentary Debates Using Applied Thematic Analysis’ (2019) 18 Qualitative social Work 6
\textsuperscript{669} ibid
participants from different CPS and MPS offices who had never worked with the researcher to writing and asking neutral questions. The researcher implemented the above measures to avoid deviation from the truth and to ensure that the study was credible given that some of the participants were her colleagues.

In conclusion, Connell, Lynch and Warring highlight that the limitations of qualitative research partially depends on the researcher’s standpoint given that the constraints could be easily regarded as the inherent strengths of the methodology.\textsuperscript{670} As previously discussed in Chapter 3, (section 3.2), given that the researcher’s epistemological assumption recognizes that multiple realities exist, her standpoint enabled her to conduct the study from a phenomenological perspective after implementing several measures to minimize the research limitation of bias which resulted in the study generating rich data.

\textit{Potential Unequal Power Balance}

As previously discussed in Chapter 3, (section 3.2), the researcher was aware that her role as an interviewer might result in an unequal power balance. Therefore, Haworth suggests that in police interviews, the roles of participants are unequal in relation to the distribution of power.\textsuperscript{671} Further, Karnieli-Miller and Strier stress that during the

\textsuperscript{670} Julia Connell, Colin Lynch and Peter Waring ‘Constraints, Compromises and Choice: Comparing Three Qualitative Research Studies’ (2001) 6 Qualitative Report 4

\textsuperscript{671} Kate Haworth ‘The Dynamics of Power and Resistance in Police Interview Discourse’ (2008) 17 Discourse and Society 6

<http://publications.aston.ac.uk/16409/1/Dynamics_of_power_and_resistance_in_police_interview.pdf> accessed 13 March 2019
personal collection of data, the aim of the interviewer is to create an environment that is welcoming and non-threatening environment in which the interviewees are willing to share personal experiences and beliefs.\textsuperscript{672} Additionally, Karnieli-Miller and Strier emphasise that an unstructured, informal, anti-authoritative, and non-hierarchical atmosphere can fuel the feeling of intimacy via which the qualitative researcher and participants establish their relations in an atmosphere of power equality.\textsuperscript{673}

Given the above observations, in conducting the interviews, the researcher was aware that as an experienced employee of the CPS who has been employed for fifteen years given her institutional status, her role as an interviewer may be perceived as controlling. Consequently, to maintain the balance of power and control between herself as the interviewer and the participants, the researcher implemented five strategies to ensure that the participants disclosed information without challenging the interviewer.

The strategies, (discussed in detail in Chapter 3, section 3.2), are establishing a rapport with the participants, listening attentively to their responses, being empathetic, seeking clarifications in a sensitive manner and not being judgmental. The strategies were significant because, given that the participants had institutional status too as investigative and prosecutorial law enforcement officials, there was a risk that the dynamics of the discourse could have been affected by their institutional roles and relative knowledge on the research topic. Consequently, Haworth argues that factors such as the institutional roles of participants, the discursive roles assigned to them

\textsuperscript{672} Orit-Karnieli-Miller and Roni Strier ‘Power Relations in Qualitative Research’ 2 2009 Qualitative Health Research

\textsuperscript{673} ibid
and their relative knowledge are factors which can affect the dynamics of power and resistance in a discourse.\textsuperscript{674}

\textbf{The population sample is confined to the London region of the UK jurisdiction}

The third limitation is that the population sample is confined to the London region of the UK jurisdiction. The researcher has therefore addressed the research issue as it affects London police officers and prosecutors. The researcher makes it clear that she has confined her findings to the London region of the UK jurisdiction because 58 out of the 63 law enforcement officials resided in London. The prosecutors and the police officers who took part in this study are based in different MPS and CPS London offices. Consequently, the viewpoints of the participants are reflective of the police officers and the prosecutors who work in different regional London offices of the MPS and the CPS.

Given that the population sample primarily consists of police officers and prosecutors, the views of the participants are not a national representation but rather, a representation of a selected sample of UK law enforcement officials. Consequently, it must be kept in mind that the conclusions drawn from the thesis reflects the views of only a cross section of London police officers and prosecutors and their results must be viewed as such. Nevertheless, the sample consisted of police officers and prosecutors from London departments of the MPS and the CPS and the data provided new insight to issues faced by both police officers and officers of the CPS in the investigation and prosecution of cyberstalkers.

The participants were recruited on a voluntary basis. Although some of the participants had different work backgrounds such as extradition, domestic violence, serious organised crime, cybercrime and sexual offences, they shared common views on the factors that hinder the investigation and prosecution of cyberstalkers.

The researcher stopped interviewing when theoretical saturation was reached. This indicated that the participants had certain commonly held views and at this point that no new insights were coming through the interview data.

**Representatives of the ISPs did not take part in the study**

A fourth limitation is that the researcher could not contact Google, Facebook or Twitter officials as there was no apparent means of contacting representatives of the ISPs directly for research purposes. Consequently, the subjective views of the Facebook and Twitter officials were not obtained.

Gul and Ali highlight that it might be a challenge to recruit and retain research participants. Therefore, they argue that an understanding of challenges and the issue that hinder the recruitment and retention of participants will enable researchers to devise strategies to overcome the barriers.

---

676 ibid
Given the above observations, the researcher acknowledges that it was unrealistic in anticipating that representatives of the ISPs would participate in the study.

5.8 Future Research

It has been highlighted that in the last decade, researchers, law makers, policy officials, and law enforcement agencies have focused on cyberstalking. Vasiu and Vasiu however suggest that although there is an extensive body of literature on the topic which identifies cyberstalking as a very serious problem, cyberstalking is nevertheless, not examined adequately in light of the rapidly evolving technologies which give perpetrators unprecedented capabilities.

There is currently no universal definition of cyberstalking. From a law enforcement perspective it is arguable that the lack of a universal definition of cyberstalking indicates that cyberstalking is not perceived to be a grave criminal behaviour justifying the regulation of the conduct via legislation. Griffiths therefore highlights that cyberstalking will only be considered a serious deviant behaviour when the conduct crosses over to physical stalking.

Against the above background, further research is required because there has not been much research focus on cyberstalking in comparison to stalking. To this effect, Vasiu and Vasiu argue that although some research has been conducted on

---

680 Bradford Reynolds, Billy Henson and Bonnie Fisher, ‘Stalking In the Twilight Zone: Extent of Cyberstalking Victimization and Offending Among College Students, Deviant Behaviour (2012) 33 (1)
cyberstalking in the last decade, more research is required to examine the cyberstalking phenomenon in light of technological advancements.681

From a risk assessment perspective, the findings of the current research indicate that there is a requirement for further research in this area based on a population sample comprising of law enforcement officials to investigate why cyberstalkers breach restraining orders and if anonymous cyberstalkers may be risk assessed based on their digital footprints. The findings of this research demonstrate that the police officers and prosecutors encounter several problems in the investigation of cyberstalkers that are magnified if the cyberstalkers cannot be risk assessed.

From a domestic violence perspective, the current study provides evidence that insinuates that lack of disclosure by domestic violence cyberstalking victims especially under reporting, can frustrate police officers and prosecutors in the investigation and prosecution of cyberstalkers. Hence, Maran and Varetto’s investigation of the motives of victims to report stalking and cyberstalking incidents implicitly to the police revealed that under reporting was a law enforcement issue.682 From a geographical perspective, Maran and Varetto’s report found that victims in larger cities were less likely to report offences than victims in smaller cities.

From a cultural perspective, the findings of this research reflect the views of DeMatteo and his colleagues that there is a varied perception of cyberstalking.683 However,

682 Daniela Maran and Antonella Varetto ‘Motives to Report Stalking to the Police:’ A Comparison between a Large City and Small Town in Italy (2017) 26 Journal of Maltreatment, Aggression and Trauma 5
the research findings unlike the findings of DeMatteo and his colleagues, do not identify areas of disagreement between public perception and statutory case law or the number of participants who were of the view that cyberstalking should be treated as a distinct offence from stalking. This is because this study was based on a smaller sample size which consisted of police officers and prosecutors whereas DeMatteo’s study comprised of a national sample of 303 participants who completed an online survey and demographic questionnaire which covered the participants perceptions about the scope of cyberstalking as a crime in addition to other matters.684 A significant law enforcement aspect of DeMatteo’s study is that it illustrates that the US public preferred other means of penalizing cyberstalkers to the imprisonment of cyberstalkers whereas the findings of this study provided data on the prosecution of cyberstalkers and revealed the perceived factors which hinder police officers and prosecutors in the investigation and prosecution of cyberstalkers.

In summary given that cyberstalking is an aspect of cybercrime, it is evident from the study as previously discussed in Chapter 4, section 4.3.5 that the inability of police officers to risk assess anonymous cyberstalkers is a factor which hinders them from identifying, monitoring and managing the risks posed by certain cyberstalkers.

It is also evident from the study that lack of evidential disclosure by domestic violence cyberstalking victims can hinder police officers and prosecutors from bring offending cyberstalkers to justice. This is more so if the behaviour of victims prevents them from realising that they are in danger from anonymous cyberstalkers especially because

684 ibid
due to lack of knowledge on cyberstalking victimisation, they are oblivious to the potential risks that they face which could lead to fatalities. More research is therefore required in this area to assist policy makers in implementing the correct measures with a view to ensuring that strategies are developed to unmask the identities of anonymous cyberstalkers with a view to bringing them to justice. Additionally, research is required on how the evidential issue of lack of disclosure by domestic violence cyberstalking victims can be tackled with a view to risk assessing and managing the risks to victims.

5.9 Reform

The issue of cyberstalking is an aspect of cybercrime that is currently reported by the UK media albeit in relation to hate crime and the online victimization of politicians or celebrities especially. Hence Mason highlights that the former Prime Minister Theresa May ordered an inquiry into the intimidation of Members of Parliament during the last general election. From a celebrity perspective, on 12 September 2019, BBC One broadcast a moving documentary by Jesy Nelson a member of the UK girl band Littlemix who has been a victim of cyberbullying for many years. In the documentary, Ms Nelson narrated the nature of the victimisation she suffers, the impact on her health and the coping strategy that she has implemented to survive the victimisation. In the documentary, Ms Nelson revealed that she attempted suicide to escape her ordeal and was speaking out to help other victims. The documentary generated a lot of public debate on cyber bullying and cyberstalking. Hence, Pandey highlights how the

documentary enlightens victims on how to cope with cyber bullying and cyberstalking implicitly.\textsuperscript{686}

Given that the findings of this study indicate that UK police officers and prosecutors share the perception that they will encounter several perceived problems in the investigation and prosecution of cyberstalkers, the researcher makes several recommendations for the government, MET, CPS and the EU to implement best practices and quintessential policies with a view to tackling the identified perceived difficulties.

The researcher has a strong law enforcement ground for proposing the recommendations listed below given that the study was based on the subjective and varied views of experienced law enforcement officials who identified the several problems that they will encounter in the prosecution of cyberstalkers.

Against this background, the researcher makes the recommendations listed below for the implementation of best practices and model policies.

\textbf{5.10 Recommendations for the Government}

\textbf{5.10.1 Creation of a centralised cyberstalking unit within the existing cybercrime units}

The findings of the study highlight that a separate cyberstalking unit staffed with computer experts is required to facilitate international cooperation. The researcher therefore recommends that a centralized body be established within existing specialised cyberstalking units with a view to ensuring that law enforcement officials obtain the information, assistance and guidance that they require in the prosecution of cyberstalkers. It is anticipated that the creation of a centralized cyberstalking unit staffed with officials who have specialist knowledge on cyberstalking will afford UK police officers the opportunity to liaise directly with computer experts on cyberstalking via telephone or email correspondence during the investigation process.

The National Cyber Crime Unit is the primary body tasked with providing a response to cybercrime in the UK.\textsuperscript{687} It has been highlighted that the unit works with the Regional Organised Crime Units, the Metropolitan Police cyber Crime Unit, government and international law enforcement.\textsuperscript{688} It would appear that the National Cyber Crime Unit was established to collaborate with partners with a view to investigating the most serious incidents of cybercrime and coordinating a national response to the previously identified common cyber threats. It is therefore debatable whether cyberstalking will be recognized as a common cyber threat.

In the UK, the National Crime Agency set up in the year 2013 as a non-governmental law enforcement organization currently deals with cybercrime as an aspect of serious organized crime\textsuperscript{689}. The organization tackles cybercrime from a consumer perspective and highlights seven common cyber threats ranging from phishing to key logging.

\textsuperscript{687} ibid
\textsuperscript{688} ibid
\textsuperscript{689} ‘National Crime Agency’ (NCA, 2017) <www.nationalcrimeagency.co.uk> accessed 21 January 2018
which the agency specifically investigates. Given that cyberstalking is not listed as one of the common cyber threats, the researcher recommends that a centralised cyberstalking unit should either be created within the National Crime Agency or independent of any existing governmental institution. The researcher further recommends that the units are equipped with experienced cybercrime officials who will offer UK police officers assistance in obtaining, preserving and analysing the digital evidence that they require in the prosecution of cyberstalkers.

5.10.2. Increasing public awareness on cyberstalking via government participation in the annual UK National Stalking Awareness Week

The researcher recommends increasing public awareness on cyberstalking via government participation in the annual UK National Stalking Awareness Week. From a comparative perspective, a measure which was adopted in the US to combat stalking and arguably cyberstalking is the annual broadcast of the presidential proclamation of the National Stalking Awareness month to commence the yearly event. To this effect in January 2015, the eleventh observance of the National Stalking Awareness Month was marked on a national and local level. This event resulted in several agencies, individuals and groups across the US engaging in various innovative activities to commemorate the day.\(^\text{690}\) The most recent proclamation was signed on January 2016 by Barak Obama as the previous president of the United States.\(^\text{691}\)


In the UK, an equivalent National Stalking Awareness Week was started in the year 2011 with a view to raising awareness on the behaviour of stalking and the protection of victims and to assist in the training of professionals on the new legislation. The researcher recommends that the UK government adopts a similar approach to the US government when opening the UK National Stalking awareness week that commences annually in April. This recommendation will ensure that there is a governmental input in the annual UK National Stalking week thereby, boosting the confidence of victims and members of the public in the government efforts to tackle stalking and cyberstalking implicitly.

3 The creation of a single definition for cyberstalking

The creation of a single definition for cyberstalking is required as there is currently no single specific definition for cyberstalking in the UK. Despite the two new offences which were created under the amended PHA, the limitation of the new legislation is that s2 (3) of the PHA does not expressly define cyberstalking but rather highlights examples of stalking activities which implicitly encompasses activities that constitute cyberstalking. Hence, her Majesty’s Inspectorate of Constabulary and her Majesty’s Crown Prosecution Service Inspectorate highlighted that there is no single accepted definition of stalking which implicitly includes cyberstalking. The inspectors made their observation from a perspective which demonstrates that there is a connection between the lack of a clear definition for stalking and the low number of reported crimes and prosecutions in the UK.

---


Given that the research participants gave different definitions for cyberstalking, the researcher further recommends that the PHA should be expanded to include a specific offence of cyberstalking which will make it easier for police officers and prosecutors to establish that an offence has been committed. In effect, if the PHA is expanded to specifically include cyberstalking, it will enable UK police officers and prosecutors to arrest and charge perpetrators for the specific offence of cyberstalking as opposed to the similar but different offences of harassment and stalking.

3 The provision of resources

The researcher recommends that resources in terms of finance, tools and manpower should be provided to equip police officers in the investigation of cyberstalkers. This is more so because it has been highlighted that the UK government is to invest £1.9 billion in new automated cyber security defences and further highlighted that this was an indication that the UK government intended to enhance cyber security and protect public institutions and ministries. Consequently, Patel and Elgot emphasise that due to the fact that the growing online threat was putting national and personal security at risk, the former chancellor Philip Hammond had announced that the financial resources will be utilised for three purposes. The purposes are to protect citizens and businesses by enhancing automated defences, to assist the cyber security industry and to prevent attacks from offenders. Given the observations, it is debatable whether cyberstalking as an aspect of cybercrime will be prioritized as a serious

---

694 Alastair Paterson ‘UK Government Gets Serious About Cybercrime’ (Huffington, 2016) <www.huffington.co.uk/alastair-paterson/uk-government-gets-serious> accessed 22 January 2018

695 Anushka Patel and Jessica Elgot ‘Philip Hammond to Spend £1.9bn Fighting Cyberattacks’<www.theguardian.com/technology/nov/1/philip-hammond-to-spend-extra-1.9bn-fighting-cyber-attacks> accessed 22 January 2018
offence hence the recommendation for resources to be provided to equip the police officers in the investigation of cyberstalkers specifically. It is anticipated that such a measure will enable police officers to effectively investigate the perpetrators.

In light of the above, it is arguable that cyber security is the primary focus of the government as opposed to cyberstalking due to the fact that in the current political climate, cyber security is geared towards protecting national security and public safety as opposed to cyberstalking which could be perceived as an aspect of cybercrime which merely leads to the invasion of an individual’s privacy. This observation is buttressed by the fact that it was recently reported that Ciaran Martin the UK head of the National Cybersecurity Centre has warned that a major cyber-attack in the UK which could disrupt British elections and infrastructure is inevitable.696 The observation was made from a perspective which highlights that such a national attack is anticipated in the next two years.

5.11 Recommendation for the Police

5.11.1 Provision of training

The research findings indicate that a lack of trained police officers can constitute an impediment to the investigation of cyberstalkers. The researcher therefore suggests

---

696 Ewen MacAskill, ‘Destructive act on UK a matter of ‘when not if’ warns cyber chief’ Guardian (London, 22 January 2018) 1
that police officers and staff at the front line should be given in depth, mandatory training on how to investigate cyberstalkers.

The training should highlight the impact of cyberstalking on victims to ensure that police officers when investigating cases and the judiciary when sentencing cyberstalkers fully, appreciate the adverse impact that cyberstalking has on the lives of victims. In effect, the training should also address the legislative and evidential and extradition requirements that need to be satisfied in the prosecution of cyberstalkers.

From the perspective of liaising with other organizations, the researcher recommends that the Metropolitan Police Service addresses the issue of lack of police training by relying on the support of relevant private organisations and charities to train police officers. Against this backdrop, Miller suggests that training, education and a willingness to collaborate are measures which can address the problem of a limitation in police response to the issue of cyberstalking.

5.11.2. Enhance police awareness on the risk assessment of victims and cyberstalkers

The researcher recommends that the head of the National Police Chief’ Council lead on stalking and harassment should introduce measures which will enable police officers to identify, monitor and manage the risks posed by anonymous cyberstalkers especially to victims. The researcher recommends that such measures should include

---

698 ibid
the provision of specialist risk assessment training for all police officers which will be linked to their professional development. The researcher also recommends that an aspect of the specialist training should focus on the risk assessment of mentally ill cyberstalkers who require medical assistance to enable police officers to promptly identify such offenders on arrest.

5.11.3. Recruitment of more staff

Given that the research found that shortage of manpower and the allocation of unmanageable caseloads were investigative issues, the researcher recommends that the Metropolitan Police Service takes prompt steps to ensure that more police officers are recruited. The significance of the recommendation is that it will ensure that there are enough police officers to investigate cyberstalkers effectively, follow up on initial complaints and complete the risk assessments of victims with a view to protecting them.

5.11.4. Continued Strengthening of the Single Point of Contact System to promote risk the risk assessment of victims

To ensure that cases are effectively progressed, the researcher recommends that the single points of contact regularly liaise with one another with a view to bringing offenders to justice. From a performance monitoring perspective, the researcher recommends that the existing Single Points of Contact (SPOC) should introduce a system for monitoring performance levels across all areas in order to identify cases that were not successfully prosecuted after consultation with the SPOCs and to
establish solutions to identified problems. This recommendation will ensure that future cases are successfully prosecuted if highlighted investigative issues are addressed.

In making the above recommendation, the researcher acknowledges that in 2017, the CPS and the MPS introduced a Stalking Single Point of Contact in response to Her Majesty’s Inspectorate of Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate report on the police service’s and Crown Prosecution Service’s approach to tackling crimes of harassment and stalking.\[^{699}\] The researcher further acknowledges that since this research took place, the CPS and the National Police Chiefs’ Council have strengthened the Single Point of Contact for the investigation and prosecution of stalking offences to ensure that the police and CPS leads on stalking fully understand the requirements and expectations of the role.\[^{700}\] The researcher is further aware that the national stalking protocol requires each police force and CPS Area to appoint a single point of contact (SPOC) for stalking to enhance effective and early consultation between the police and the CPS.\[^{701}\]

The researcher additionally acknowledges that Her Majesty’s Inspectorate Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate in their critical findings of their joint report, highlighted that the SPOC should include close liaison with third-sector organisations that provide support to victims of stalking and cyberstalking implicitly.\[^{702}\] From a risk assessment perspective, the researcher further

\[^{700}\] As previously discussed, the measures were introduced following Her Majesty’s Inspectorate of Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate inspection and report
recommends that while liaising with third-sector organisations that provide support to victims of stalking and cyberstalking implicitly, the SPOC in all areas should make the risk assessment of victims a primary priority to ensure that appropriate measures are implemented to protect victims.

5.11.5 Introduce of a standardized cyberstalking incident form

To ensure that cyberstalking cases are investigated effectively, the researcher recommends that a centralised cyberstalking police incident form should be introduced for all the police forces to ensure that local intelligence on convicted cyberstalkers are collated on a database. The introduction of such a measure will enable police officers to have a centralised access to data on known offenders and will make it easier to an extent for police officers to access the relevant intelligence data on UK cyberstalkers. At the time of the study, there was no evidence of the existence of such a form.

The researcher recommends that the cyberstalking police incident form should complement the existing checklist for stalking cases which was introduced in the year 2009 as a risk identification tool.703

5.11.6 Establish a local a specialized telephone investigation unit in all police forces

To tackle the issue of investigative delays, the researcher recommends that a dedicated telephone investigation unit is created in the various police stations and that

---

a timetable is drawn up for actions to be completed with a view to speeding up the investigation process. From a domestic perspective, the researcher proposes that a specific official based at a single telephone investigative unit should be employed to analyse the phone and email data of cyberstalkers in a bid to reduce the red tape involved in this aspect of the investigation process. The researcher recommends that such a unit is introduced within the existing specialised cybercrime units with a view to introducing a consistent approach to conducting telephone investigations relating to cyberstalking.

5.12 Recommendation for the CPS

5.12.1. Provision of mandatory and refresher training

The researcher acknowledges that the CPS on 5 July 2017, announced that it will update the Stalking and Harassment e-learning and make it mandatory for all lawyers.\textsuperscript{704} To ensure that there is a consistent approach to the prosecution of cyberstalkers, the researcher recommends that the CPS continues to provide mandatory courses on the prosecution of cyberstalkers.

Additionally, the researcher recommends that the CPS provides refresher training courses at regular intervals. Currently, the CPS has online training courses which enlighten prosecutors and other employees on the legislative and evidential aspects to the prosecution of cyberstalkers since the creation of two stalking offences under the amended PHA. However, the findings of the study indicate that prosecutors will

benefit from refresher training courses on the prosecution of cyberstalkers given that the online training was not mandatory at the time of the study. This is more so given that the publication of her Majesty’s Inspectorate of Constabulary and her Majesty’s Crown Prosecution Service Inspectorate revealed that there is a danger of stalking offences being prosecuted as harassment cases.705

5.12.2. Creating the role of specialist cyberstalking Prosecutors

The findings of the study revealed that there were no specialist cyberstalking prosecutors at the time of the study and that prosecutors routinely reviewed cases on cyberstalking when required. The researcher therefore recommends that the distinct role of specialist cyberstalking prosecutors should be introduced to ensure that a consistent approach to the prosecution of cyberstalkers is promoted given the Adverse effects of cyberstalking on victims.

5.12.3. Raising staff awareness on prosecution of cross jurisdictional cyberstalking

Given that most of the cyberstalking cases which were reviewed by the participants, were domestic cases as opposed to cross-jurisdictional cases, the researcher recommends that the CPS embarks on an increased staff awareness campaign on the

prosecution of cross-jurisdictional cyberstalking to ensure that all prosecutors are equipped to review such cases from an international perspective when required.

The researcher further recommends that there should be an increased public awareness campaign on how specialist prosecutors can liaise with the ISPs and global law enforcement agencies in the prosecution of cross-jurisdictional cyberstalkers.

From an EU perspective, despite the fact that the UK is in the process of leaving the European Union, there is still a legal requirement for UK law enforcement officials to apply the relevant EU directives or regulations on the deviant behaviour of cyberstalking when required. This is more so, given that cyberstalking is a cross-jurisdictional criminal behaviour and that some countries are yet to enact legislation on the regulation of cyberstalking. The significance of the above recommendation is that if implemented, it will ensure to some extent that prosecutors adopt a consistent approach in the application of relevant EU legal measures when reviewing cross-jurisdictional cyberstalking cases amidst the Brexit negotiations.

It is important to note that the CPS recently took some measures to raise staff awareness on harassment and stalking which implicitly includes cyberstalking. To this effect on 24 January 2018, the CPS notified the London staff via email of the updated legal guidance on harassment and stalking. The guidance is significant because it statutorily defined the offences of harassment and stalking, highlighted the relevant cases laws and set out the relevant legal principles. Additionally, the guidance highlighted the police and CPS response to the Her Majesty’s Inspectorate of

---

Constabulary and Her Majesty’s Crown Prosecution Service Inspectorate report on the response of the police and the CPS to stalking and harassment.\textsuperscript{707}

Further, on 23 February 2018, the CPS additionally notified staff via email of the new guideline that has been published by the sentencing council in relation to the offence of domestic violence.\textsuperscript{708} From a cybercrime perspective, the notification was made from a standpoint which indicates that the updated domestic violence guideline is significant because it acknowledges that perpetrators can utilise information and communication technology such as the email, text, social networking sites and GPS trackers to target victims.

5.13 Recommendation for the EU

5.13.1. Enactment of an EU directive on cyberstalking

Given the cross-jurisdictional feature of cyberstalking and that the UK is still in the process of leaving the EU, the researcher recommends the introduction of an EU directive requiring member states to assist in the investigation of cross-jurisdictional cyberstalkers. The researcher anticipates that the introduction and implementation of such a specific legislative measure will ensure that the member states play a more significant role in the investigation of cross-jurisdictional cyberstalkers resident within and outside the EU respectively. As discussed below from a legislative perspective,

\textsuperscript{707} ‘Harassment and Stalking London Legal Guidance’ (CPS, 2018) <www.infonet.cps.gov.uk/infonet_live/announcements/pages/sentencing> accessed 23 February 2018

the researcher acknowledges that the EU have taken certain measures to criminalise cybercrime and stalking which implicitly includes cyberstalking offences.

From a regulatory perspective, the European Union directive on the European Protection Order is the only European legislative measure which specifically addresses stalking.\textsuperscript{709} It is arguable that the directive encompasses the related criminal behaviour of cyberstalking. The directive stipulates that domestic criminal protection orders are applicable in other member states across the European Union. Although the European Protection Order constitutes a legal basis in the European Union which enables a member state to recognize a criminal protection order granted in another member state, its effectiveness has been criticized on two grounds. The first ground is that it has very restricted applicability given that only stalking victims who move to another member state and who are still in danger can benefit from the European Protection Order.\textsuperscript{710} The second ground is that it does not alter the fact that there are significant variations in the types of protection that are available for stalking in the different states within the European Union.\textsuperscript{711}

From the perspective of preventing violence against women on 21 May 2011, the Council of Europe introduced the Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence. The convention is significant because it categorically highlights stalking as a criminal behaviour. Specifically, Article 34 of the convention requires states to regulate stalking via

\textsuperscript{710} ibid
\textsuperscript{711} ibid
legislative measures and implicitly, cyberstalking which is a hybrid of stalking.\textsuperscript{712} Van der Aa and Romkens highlight that in defining stalking, the explanatory report to the convention explains that spreading untruthful information online can constitute stalking.\textsuperscript{713}

From a historical perspective, the researcher acknowledges that in 2001, the Council of Europe adopted the Convention on Cybercrime.\textsuperscript{714} It was anticipated that the decision of the Council of Europe to draft an international Convention on Cybercrime would promote the investigation and prosecution of cybercrime on a global scale. The Convention on Cybercrime is a significant law enforcement strategy because it addresses the criminalization of cybercrime, the application of local steps to enhance the investigation and prosecution of cybercrime and the grounds for the investigation and prosecution of cybercrime.\textsuperscript{715}

From a critical perspective, the convention makes no reference to cyberstalking as an aspect of computer crime. However, Articles 2, 3, 4 and 5 of the convention regulate some stalking behaviours that can incorporate global cyberstalking.\textsuperscript{716} The Articles deal with instances when a stalker illegally accesses the computer of a victim, illegally intercepts the electronic communication of victims, intentionally destroys the data stored on the computer of a victim and vandalises the computer of a victim. From an international law enforcement perspective, this four-fold approach to expressly

\textsuperscript{712} ‘Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence’ (COE, 12 April 2011) <www.rm.coe.int/168046031c> accessed 15 January 2018
\textsuperscript{715} Suzanne Van der Aa, ‘International (Cyber) Stalking, Impediments to Investigation and Prosecution’ (Pure, 1 January 2011) <www.pure.uvt.nl/ws/files/1310512/Aa_International_cyberstalking_110216_posprint_embargo_1_y.pdf> accessed 10 August 2018
criminalizing stalking behaviours which implicitly constitute cyberstalking offences is a step in the right direction.

From an academic perspective, Maple and Lang emphasise that there is a need to protect the rights of vulnerable cyberstalking victims in particular at an EU level given the effects of cyberstalking on victims, the anonymous nature of the offence and the fact that that cyberstalkers can victimise from behind closed doors. Consequently, Maple and Lang question why cyberstalking was not included in the list of crimes that were highlighted by the European Commission after it implemented on 18 May 2011, its proposal for directive 2012/29/EU which will define minimum standards on the rights, support and protection of victims of vulnerable crimes. Notably, Maple and Lang argue that the EU has a special responsibility to victims of cyberstalking given the cross-border feature of the crime and the fact that the ISPs and website owners especially may be situated in different member states. Hence, it has been highlighted that Brexit might afford the government an opportunity to act given that at present, social-media companies are not currently liable primarily as a result of an EU directive that classifies them as merely hosts of online contents.

5.13.2. The creation of a universal definition for cyberstalking

---

718 On 12 September 2012 and 4 October 2012 respectively, the directed was adopted by the European Parliament and by the Council of ministers
719 ‘Chuka Umunna Fears Being Pushed Off a Tube Platform’ (BBC, 13 December 2017) <www.bbc.co.uk/news/uk-politics> accessed 14 December 2017
There is currently no universal definition for cyberstalking despite the fact that in the year 2010, the European Commission analysed the laws on stalking in the European member states.\(^\text{720}\) The fact that the European Commission did not specifically address the related issue of cyberstalking in its analysis, arguably indicates that cyberstalking is yet to be deemed a distinct serious deviant behaviour warranting criminalization on an EU scale.

The researcher acknowledges that Article 34 of the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence obliges signatory states to criminalize stalking and cyberstalking implicitly.\(^\text{721}\) The convention came into force in 2013 and is the only convention that refers to stalking. Given that the convention does not specifically refer to cyberstalking and that members states have found to hold different perceptions of what constitutes stalking, the researcher recommends that there should be a universal definition of cyberstalking by the EU. It is arguable that the EU can introduce an EU directive on cyberstalking especially which will require member states to enact domestic legislation to give effect to the terms of the cyberstalking directive. At the time of the study, Article 34 of the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence appeared to be the only directive which has so far been introduced by the EU with a view to harmonising the law on stalking and cyberstalking implicitly.

\(^{720}\) ‘Feasibility Study to Assess The Possibilities, Opportunities and Needs to Standardise National Legislation on Violence Against Women, Violence Against Children And Sexual Orientation Violence’ (Europa, 2010)

In light of the above, from a critical perspective, Van Der Aa asserts that the wordings of article 34 of the Convention are poor particularly concerning their stress on the consequences of the stalking for the victim. Van Der Aa argues that the requirement that the stalking should have caused the victim to fear for his or her safety is an especially high threshold that leaves victims unprotected. Further, Van Der Aa emphasises that although the members do not appear to be in violation of article 34, their perception of what constitutes stalking sometimes digresses from the intentions of the Convention.

The researcher anticipates that the creation of a universal legislation will promote legislative uniformity across the various global jurisdictions. Such a global legislative measure is required in light of the fact that physical proximity is not a barrier to cyberstalking.

5.14 Conclusion

The research in this thesis described the qualitative investigation of the perceptions of London Based police officers, prosecutors and UK law enforcement officials regarding the factors that frustrate them in the investigation and prosecution of cyberstalkers. In doing so, the research further sought to establish what these legal professionals understand to be the threshold for distinguishing rudeness, abuse and unpleasant comments on the internet from cyberstalking. Additionally, the research sought to

723 ibid
identify the perceived challenges that participants believe impede the risk assessment of cyberstalking victims.

The findings from this research demonstrate that police officers and prosecutors identify six law enforcement difficulties factors which will potentially hinder them in the investigation and prosecution of cyberstalkers. The findings also reveal that police officers and prosecutors identified several perceived thresholds of acceptable behaviour online and these were dependent on the area of their own professional practice. Finally, the results of the study reveal that the anonymity afforded to cyberstalkers by the internet is an impediment to the risk assessment of victims and cyberstalkers.

The research is unique because the findings are based on the subjective viewpoints of experienced police officers and prosecutors practicing in the UK. The results reported in this thesis matter because from the perspective of victims, they highlight that if the identified investigative problems are not addressed by the relevant stakeholders, the problems could result in cyberstalkers evading justice and also, both victims and cyberstalkers not being properly risk assessed.

The research contributes five important findings which add knowledge to the field of cyberstalking as an aspect of cyber enabled crime. The findings are linked to the anonymity of cyberstalkers as a hindrance to the risk assessment of victims, under reporting as an impediment to the risk assessment of victims and victim behaviour as an obstacle to the prosecution of cyberstalkers in domestic violence cases.
The first finding asserts that police officers cannot risk assess victims with a view to protecting them if they are being harassed by anonymous cyberstalkers whose identities cannot be revealed due to a lack of specialist knowledge on how to unmask their identities. The participants additionally revealed that police officers cannot risk assess anonymous cyberstalkers with a view to establishing the risks that they pose to victims if their identities cannot be unmasked. Importantly, the research found that the issue of anonymity has been exacerbated by the fact that some anonymous cyberstalkers use unregistered pay as you go mobile phones and SIM cards to avoid detection thereby, evading prosecution.

The second finding that was made by the research is that the issue of under reporting hinders police officers investigating and risk assessing victims because police officers can only investigate offenders if they are notified of cyberstalking incidents via formal complaints. The finding is relevant because it draws attention to the fact that under reporting results in police officers not being able to risk assess victims and cyberstalkers if they have not been made aware that offences have been committed by offenders.

The third relates to the behaviour of victims in cyberstalking cases involving domestic violence which can lead to various issues which ultimately hinder the successful investigation and prosecution of cyberstalkers. The behaviours include; disclosure issues, the refusal of victims to attend court, the decision of victims to cross communicate with offenders and the decision of victims to have intermittent relationships with offenders.
In addition to the above, the research found that police officers and prosecutors shared the perception that legislative difficulties, lack of knowledge and training, lack of resources, risk assessment challenges, evidential challenges and victim behaviour are factors which frustrate them in the investigation and prosecution of cyberstalkers. This finding adds to knowledge because it confirms from a dual investigative and prosecutive perspective that police and prosecutors in London hold the view that the identified difficulties need to be resolved to enable them bring offenders to justice, protect victims and deter offenders.

The fifth finding that was made by the research is that there are various thresholds of acceptable behaviour online and how it is distinguished from cyberstalking. The finding is relevant because it reveals that police officers and prosecutors consider cyberstalking as criminal behaviour which can be associated to a single threshold of acceptable online behaviour. The finding adds to this field of knowledge because at the time of the research, no study had been carried out on the joint perception of police officers and prosecutors on the threshold of acceptable online behaviour which distinguishes and cyberstalking as a cyber-enabled aspect of cybercrime.

In sum, this thesis has, through the research context highlighted key perceived, investigative, problems namely anonymity, under reporting and victim behaviour which prevent police officers and prosecutors from risk assessing victims and cyberstalkers with a view to protecting victims and gauging the risks posed by cyberstalkers. Consequently, this thesis argues that it is vitally important for the relevant stakeholders to implement measures, such as those suggested in this thesis that will address the
highlighted difficulties and smooth the way to successful investigation and prosecution of this cyber-enabled crime.

Bibliography

Books


Caven-Clarke, S *Cyberbullying a Focus On* (1st edn, Booklife Publishing 2018) 8.


Eck J, and Clarke R’ ‘Classifying common police problems: A Routine Activity Approach’ in Martha Smith and Derek Cornish (Eds) *Situational Crime Prevention* (Criminal Justice Press 2006)


Hayes S, ‘Cyberbullying is a Serious Problem’ in Lauri Friedman (Ed) Cyberbullying (Greenhaven Press 2011) 11.

Hogan, S 7 ‘Cyberbullying is worse than Traditional Bullying’ in Lauri Friedman (Ed) Cyberbullying (Greenhaven Press 2011) 11.


Hyson C, Cybercrime (Franklin Watts Publishers 2010) 1.


Katz A, Cyberbullying and E-Safety What Educators and Other Professionals Need to Know (1st edn, Jessica Kingsley Publishers 2012) 1.


McQuade S, Understanding *and Managing Cybercrime* (Greenwood Press 2006) 1.

McQuade S, Encyclopaedia of *Cybercrime* (Greenwood Press 2009) 7.


Sanchez, L ‘Cyberbullying should be treated as a crime’ in Lauri Friedman (Eds) *Cyberbullying* (Greenhaven Press 2011) 34.


**Journal Articles -Print**


Bhavna Arora ‘Exploring and Analyzing Internet Crimes and Their Behaviours’ (2016) 8 Perspectives in Science.


Christopher Benitez, Dale McNiel and Renée Binder ‘Do Protection Orders Protect?’ (2010)


Louise Corti, Day and Blackhouse, ‘Confidentiality and informed consent: issues for consideration in the preservation of and provision of access to qualitative data’ (2000) 1 Qualitative Social Research 3


Apopiah Namageyo-Funa, Marylen Rimando, Andrea Brace, Richard Christiana, Tiffany Fowles, Tianiese Davies, Lourdes Martinez and Diadrey-Anne Sealey ‘Recruitment in qualitative research: lessons learned during dissertation sample recruitment’ (2014) 19 The Qualitative Report 4


Thomas Holt, Sarah Fitzgerald, Adam Bossler, Grace Chee and Esther Ng ‘Assessing the Risk Factors of Cyber and Mobile Phone Bullying Victimization in a Nationally Representative Sample of Singapore Youth’ (2014) 60 International Journal of Offender Therapy and Comparative Criminology 5.


Steven Krauss, ‘the qualitative research paradigm and meaning: Making a primer’ (2005) 10 Qualitative Report 4.


Neil MacEwan ‘the new stalking offences in English law: will they provide effective protection from cyber stalking?’ (2012) 10 Criminal Law Review,


Daniela Maran and Antonella Varetto ‘Motives to Report Stalking to the Police: A Comparison between a Large City and Small Town in Italy’ (2017) 26 Journal of Maltreatment, Aggression and Trauma 5.


Reid Melroy and Alan Felthouse ‘Introduction to this issues: International Perspectives of Stalking’ (2011) 29 Behavioural Science and the Law 2.


Fawn Ngo and Raymond Paternoster ‘Cybercrime Victimization: An Examination of Individuals and Situational Level Factors’ (2011) 5 International Journal of Cyber Criminology 1.


Nicolle Parsons-Pollard, ‘Cyberstalking laws in the United States: Is there a need for uniformity?’ (2010) 46 Criminal Law Bulletin 5,


Waleed Al - Rahmi, Noraffandy Yahaya, Mahdi Alamri, Nada Aljarboa, Yusri Bin Kamin and Fahad Moafa ‘A Mode of Factors Affecting Cyberbullying among University Students’ (2018) 7 IEEE.


Elizabeth Wick, Craig Nagoshi, Randy Basham, Catheleen Jordan, Youn Kyoung Kim, Anh Phuong Nguyen and Peter Lehmann ‘Patterns of Cyber Harassment and


Online journals


Websites

Action against Hate the UK Government’s for Tackling Hate Crime Two Years On’ (Government, 18 October 2018)  


Convention on Convention on Preventing and Combating Violence against Women and Domestic Violence (12 April 2011, COE)

‘Convention on cybercrime’ (Europa, 23 November 2001)

‘Council of Europe Convention on preventing and combating violence against women and domestic violence’ (COE, 12 April 2011)

‘CPS Response to HMIC/HMCPSI Joint Thematic Inspection of Harassment and Stalking Offences’ (CPS, 5 July 2017)


David Harvey, ‘Cyberstalking and internet harassment: what the law can do’ (Victimsorg, 1 January 2003) <http://victimsofcrime.org/docs/Information%20Clearinghouse/Cyberstalking%20and


‘Hampshire police stalking clinic praised in inspection’ (Portsmouth, 5 July 2017)  

Janet Hitchcock, ‘Cyber stalking and law enforcement’ (Police Chief Magazine 2003)  


‘Issues on paper crime affecting personal safety, privacy and reputation including cyberbullying’ (Law Reform Commission, 2014)  


‘Prosecution and case management Charging and case preparation’ (College of Policing, 20 June 2017)
Rachel Kilean, John Goddard, Gillian McNaull, Shaghayegh Beigi, Alexandra Born, Stephanie Johnston and Jaclyn Walters ‘Review of the need for stalking legislation in Ireland’ (Queen University Belfast, 2016)

Alair Kilp ‘The Positive and Negative Function of Perceptual Bias in Interpersonal Relations’ (2011) 14 ENDC Proceedings (KSK, December 2012)


‘Malicious Communications Act’ (GOV, 1988)

Mike McGuire and Samantha Dowling ‘Cybercrime: A review of the evidence Chapter 1: Cyber-dependent crimes Home Office Research Report 75’
(Govt, 7 October 2013)


Felis Stalder ‘The logic of networks. Social landscapes Vis-a Vis the space of flows’ (CTheory, 19 February 2020)

Razieh Tadayon Nabavi ‘Bandura’s Social Learning Theory & Social Cognitive Learning Theory’ (Researchgate, January 2012)

‘New stalking legislation helps to bring more prosecution as CPS and ACPO launch protocol to improve services to stalking’ (CPS, 11 September 2014)


‘New stalking legislation helps to bring thousand more prosecutions as CPS and ACPO launch protocol to improve service to victims’ (CPS, 2012) <http://www.cps.gov.uk> accessed 17 August 2016.


‘Practice advice on investigating stalking and harassment’ (ACPO, 2009).  


‘Protocol on the appropriate handling of stalking cases between the Crown Prosecution Service and ACPO’ (CPS, 2014)  

Kimberley Prost, ‘Breaking down the barriers, international cooperation in combating transnational crimes’ (OAS, 2007).


‘Understanding cybercrime: Phenomena, challenges and response’ (ITU, September 2012)


Newspaper Website

Nick Allen, ‘Hollywood accused of hypocrisy over Harvey Weinstein’s sexual harassment allegations’ (The Telegraph, 12 October 2017)

Jennifer Baker, ‘Ladies and Trolls: Should We Make Cyberbullying A Crime?’ (The Register, 5 January 2015)
<https://www.theregister.co.uk/2015/01/05/speak_your_brains_should_we_criminalise_cyberbullys_asks_ireland/> accessed 9 August 2018

Luke Barnes,’ Girls aloud singer Nicola Roberts bitter ex-boyfriend bombarded her with messages from dozens of fake Twitter and Instagram accounts including stabbing emojis in five year campaign of stalking’ (Mail Online, 7 May 2017)
<https://www.dailymail.co.uk/news/article-4481708/Nicola-Roberts-s-bitter-ex-bombarded-messages.html> accessed 13 August 2018

Tom Brady ‘Computer cases facing six year delay due to computer backlog’ (The Independent, 1 November 2016)


‘Facebook to hire another 3,000 people to review videos of crime and suicides’ (Belfast Telegraph, 3 May 2017) <https://www.belfasttelegraph.co.uk/business/technology/facebook> accessed 17 January 2018
‘Facebook stalker murdered ex-girlfriend’ (The Telegraph, 26 January 2012)
<https://www.telegraph.co.uk/news/uknews> accessed 25 September 2017

‘Google bows to pressure to tackle extremist’ (The Week, June 20 2017)
<https://www.week.co.uk/85809-google-bows-to-pressure-to> accessed 19 January 2018

Nicola Fifelied ‘Cyberstalker bugged Women’s Computers to Spy on Them in their Bedrooms’ (The Telegraph, 30 May 2014)

Frances Gibb ‘Pay out for YouTube star Chrissy Chambers over revenge porn’ (The Times, 18 January 2018) <https://www.thetimes.co.uk/payou-for-youtube-star-chrissy-chambers-over-revenge-pornography> accessed 23 February 2018


Jasmine Holley, ‘Girls aloud star granted life time restraining order from stalker ex’, (Entertainment daily, May 8 2017) < https://www.entertainmentdaily.co.uk/
News-girls-aloud-star-granted-restraining-order-from-stalker-ex >

Accessed 5 June 2017

Chris Johnston, Graham Russell, Sam Levin, Julia Carrie and Kevin Rawlinson
‘Disruption from Cyber-Attack Lasts For Days, Says NHS Digital - As it Happened’
(The Guardian, 13 May 2017)

Cormac. O’ Keffee, ‘New laws to combat online abuse such as bullying and revenge porn’ (Irish Examiner, 27 September 2016)
<https://www.irishexaminer.com/ireland/new-laws-to-combat-online-abuse-such-as-cyberbullying-and-revenge-porn-422963.html> accessed 9 August 2018

Alexander Martin ‘Did you know that there is a mega cybercrime backlog in Ireland? Now you do. Ireland needs 5 years to tackle it. Garda needs five years to tackle it and the help of the FBI!’ (The Register, 2016)

Anushka Patel and Jessica Elgot ‘Philip Hammond to spend £1.9bn fighting cyberattacks’ (The Guardian, 1 November 2016)
<https://www.theguardian.com/technology/nov/1/philip-hammond-to-spend-extra-1.9bn-fighting-cyber-attacks> accessed 22 January 2018
‘Police seek powers to access browsing history data of UK computer users’ 
(Guardian, 30 October 2015) <https://www.gu...> accessed 22 January 2017

Katharine Quarmby, ‘How the law is standing up to cyber stalking’ The Newsweek 

Rowena Mason ‘PM Orders Inquiry into Intimidation of MPs during General Election’ 

Andrew Rettman and Damian McElroy ‘EU data laws struck down by court ruling’ 
(The Telegraph, 8 April 2014) <https://www.telegraph.co.uk/news/worldnews/europe> accessed 30 January 2018


Radhika Sangani ‘I collapsed on the floor, ‘screaming’: Meet the YouTube star taking on Britain’s revenge porn law’ (The Telegraph, 8 July 2016) <https://www.thetelegraph.co.uk/women/life> accessed 17 January 2018


John Twomey, ‘Anti-terror chief’s blast at social media’ (The Express, 7 March 2018) <https://www.express.co.uk/news/uk> accessed 8 March 2018


Newspaper Print

Owen Bowcott and Alex Hern ‘UK and US class-action launched against Facebook and data firms’ The Guardian (London, 11 April 2018) 4

Sam Coates and Rhys Blakely, ‘May: investors must force tech giants too ban extremist contents’ The Times (London, 25 January 2018) 1

James Dean ‘Zuckerberg agrees to tighter regulation’ The Times (London, 18 April 2018) 6

Margarette Driscoll, ‘Messages that sent my girl to death’ The Sunday Times (London, 4 December 2011) 9

Andrew Gillian, ‘Clampdown on Facebook hate’ The Sunday Times (London, 26 November 2017) 1

Nicholas Hellen ‘Twitter told: stalking costs Lives, sort it’ The Sunday Times (London, 12 August 2018) 7

Mark Horn ‘Drug dealers sell openly on Facebook’ The Times (London, 18 April 2018) 6

Ewen MacAskill, ‘Destructive attack on UK a matter of ‘when not if’, warns cyber chief’ The Guardian (London, 22 January 2018) 1


Isabel Oakshot and Mark Hookham, ‘Stalkers face five years in prison’ The Sunday Times (London, 4 March 2012) 16

Ross Shan ‘Stalkers Freed due to lack of Police Training’ the Scotsman (Scotland, 10 February 2014) 1

David Smith ‘Fighting global election fraud is chief priority says Zuckerberg’ The Guardian (London, 11 April 2018) 1


Sarah-Kate Templeton ‘Hunt mulls laws to guard young online’ The Sunday Times (London, 22 April 2018) 2

Jon Ungoed-Thomas et al, ‘Cyberattack promoted on youtube’, The Sunday Times (London, 14 May 2017) 1


**Blogs**


Alastair Paterson ‘UK government gets serious about cybercrime’ (Huffington, 7 November 2016) <www.huffington.co.uk.alastair-paterson/uk-government-gets-serious> accessed 22 January 2018

Gary Shewan, ‘Stalking. Know the law, use the law’ (weblog, 18 April 2013) <www.acpo.police.uk/the police chiefs blog > accessed 11 May 2017

Reports


‘Cyber violence against women and girls a world-wide-wake-up-call. A report by UN broadband commission for digital development working group on broadband and gender’ (UN women, 24 September 2015) <www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015> accessed 13 January 2018

‘Digital Britain Final Report’
Ditch the Label: The Annual Bullying Survey 2018’ (Ditch the label, 2018)

Hate Crime Annual Report’ (CPS, October 2018)


‘Independent parliamentary enquiry into stalking law reforms’ (Dashrisk, September 20016) <http://www.dashriskchecklist.co.uk> accessed 9 March 2014


Pat Strickland and Jack Dent ‘Online Bullying and Harassment’ (Researchbriefings, 13 September 2017) <researchbriefings.parliament.uk/ResearchBriefing/Summary/CP-7967> accessed 15 December 2018


‘2014 report to congress, grant funds used to address stalking’ (US Department of Justice, January 2017) <http://www.justice.gov/ovw/page/file/932736/download> accessed 2 March 2018


445

Legal Guidance


‘The Code for Crown Prosecutors’ (CPS, 26 October 2018) 
<www.cps.gov.uk/publication/code-crown-prosecutors> accessed 15 December 2018

‘Crown Prosecution Service, (CPS, 2013) Director’s guidelines on the handling of cases where the jurisdiction to prosecute is shared with prosecuting authorities overseas’ <www.cps.gov.uk> accessed 19 October 2013

‘Crown Prosecution Service’ Guidelines on extradition’ (CPS, 2013) 
<www.cps.gov.uk> accessed 27 November 201

‘Cybercrime - prosecution guidance’ (CPS, 2017) 
<www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance> accessed 15 December 2018

‘Guidelines on prosecuting cases involving communication sent via social media’, (CPS, 2013) <www.cps.gov.uk/legal > accessed 15 June 2017


‘Harassment and stalking London legal Guidance’ CPS London staff communication (CPS, February 16 2018)


‘Practice advice on investigating Stalking and Harassment’ (ACPO, 2013) <www.acpo.police.uk/documents/crime> accessed 19 October 2013


Strategies

Cyber Crime Strategy' (Home Office, March, 2010)

Cyber Security Strategy protecting and promoting the UK in a digital World'
(Government, November 2011)

accessed 14 December 2018

‘Digital Britain Final Report’

National Cyber Security Strategy 2016-2021 (NCSS, 2016)

Appendices

Appendix One

(a) Email text of the CPS granting access to the CPS sample of prosecutors

Gateway Research Message

Ms Ori Igwe is a CPS employee who is currently studying for a PhD on the international prosecution of cyber stalkers at the Ealing Law School of University of West London under the supervision of Professor Malcolm Davies and Dr Phillip Elliot-Wright. The research has been approved by Jean Ashton who is the Area Business Manager of CPS London. The CPS has authorized Ms Igwe to interview 50 London Crown prosecutors during the course of her research. The doctoral study has also been approved by the research department of the London Metropolitan Police Force.

The research is seeking to build on the experience of Crown Prosecutors who have dealt with such cases. As part of her research, Ms Igwe is seeking to interview 50 London Crown prosecutors on an anonymous basis with a view to identifying the challenges faced by Crown prosecutors in the cross-jurisdictional prosecution of cyber stalkers. The interviews will last for approximately 20 minutes and Ms Igwe is prepared to meet with the interviewees at a time and place that is convenient for them. She has so far interviewed 35 police officers, senior members of parliament, probation officials, American law enforcement officials and Eurojust officials. The findings will be published on completion of the research and will contribute towards policy debate in this area. If you are able to help please contact Ms Igwe or her CPS mentor, district crown prosecutor.
Hi Ori,

Just to keep you updated, we have looked at your protocol, and your work seems very interesting and certainly of use to the MPS. As you are fully vetted, there should be no issues in getting you access to MPS sites, employees or data, however we may need to verify that you are indeed vetted (would you have any proof of this to send to us?) just to be sure. Both and I are currently waiting for a reply from and someone in SCD6 so that we can help you get access to the right people. If we do not receive a reply by the end of the week, I will start chasing people up. I hope that is alright.

Thanks,
Dear Colleague,

As someone who has grounded your research within the Metropolitan Police Service (MPS), I am writing to ask if you would agree to share this work with the wider police family. I am aware that some of the fruits of your work may already be in the public domain through the peer review academic route, such as publications in books or articles, but we would like to extend this.

As you may know, this December saw the launch of the national College of Policing (formerly the National Policing Improvement Agency - NPIA). The College will retain many of the original responsibilities held by the NPIA, and may lose others, but there is a strong commitment from the Home Office to improve the way policing uses research evidence:

"The [College] will strengthen the links between the police service and other organisations. It will work with universities to share and develop the underlying evidence base for policing practice. It will work with other organisations, including with the private sector to ensure that, where appropriate, the police service is able to access the very best training from outside the police service. It will work closely with international partners, to ensure the police service is able to share and access the very best thinking from across the world."

College of Policing: an Introduction (16.7.12)
In support of this mission, the MPS is changing the way it gathers, uses and shares research evidence. The MPS is working closely with the College of Policing to ensure that research knowledge is harnessed within the policing community and embedded into the way we work here in the Met. We aim to promote new research, but also encourage dialogue between policing, academia and the wider public about what works in policing.

In order to achieve this, we are working with the College to create an easily accessible repository for research papers. You may remember completing the MPS research protocol when registering your research with Corporate Development (formerly Strategy and Performance and SRAU). This document permits us to share the details of your research within the MPS, through our intranet site and internal seminars. However, we would like to take this one step further and share the research more widely. You have a few options of where the details may be shared and what is included. One, the information can be publicly available and accessed by anyone via the web. It is proposed that a table will be published in the public domain and within the policing community, with a list of research outlines, key findings, author details and PDF links to each report. Two, the information can be available only within the national policing community via POLKA; and three, your information can be made available only within the MPS, as initially agreed. In the future we will be explicit that any research completed in the MPS will be available to all those within the police community.

I have noted below a series of options for you to consider with respect to the research that you registered with us. Please could you indicate whether you would be happy for
your details and that of your research to be published, including any other conditions? Also, if publication rights make it impossible to share your findings externally, please could you provide us with an abstract and link? Leave the appropriate line displayed, deleting the others:

- I consent to my research outline, author/supervisor details and findings to be published on the public College of Policing website

- I consent to my research outline and author/supervisor details being published on the public College of Policing website, but do not consent to my findings being published. Please elaborate (e.g. awaiting clearance, time restrictions etc) The link to the findings as follows: ______________________________

- I consent to my research outline, author/supervisor details and findings to be published on a website accessible only to the national police service and associated organisations (e.g. Police Online Knowledge Area -POLKA).

- I consent to my research outline and author/supervisor details being published on a website accessible only to the national police service and associated organisations, but do not consent to my findings being published. Please elaborate (e.g. awaiting clearance, time restrictions etc). The link to the findings is as follows: ______________________________
I do not consent to my research outline, author/supervisor details or findings to be published on a website accessible outside the MPS

If we do not hear from you by 15 January 2013 we will exclude your research from the POLKA website.

Please send all responses to: research@met.police.uk

Kind Regards,

Professor Betsy Stanko
Corporate Development
Metropolitan Police Service
Empress State Building, Lillie Road,
London, SW6 1TR

Total Policing is the Met's commitment to be on the streets and in your communities to catch offenders, prevent crime and support victims. We are here for London, working with you to make our capital safer.

Consider our environment - please do not print this email unless absolutely necessary.

NOTICE - This email and any attachments may be confidential, subject to copyright and/or legal privilege and are intended solely for the use of the intended recipient. If you have received this email in error, please notify the sender and delete it from your system. To avoid incurring legal liabilities, you must not distribute or copy the information in this email without the permission of the sender. MPS communication
systems are monitored to the extent permitted by law. Consequently, any email and/or attachments may be read by monitoring staff. Only specified personnel are authorised to conclude any binding agreement on behalf of the MPS by email. The MPS accepts no responsibility for unauthorised agreements reached with other employees or agents. The security of this email and any attachments cannot be guaranteed. Email messages are routinely scanned but malicious software infection and corruption of content can still occur during transmission over the Internet. Any views or opinions expressed in this communication are solely those of the author and do not necessarily represent those of the Metropolitan Police Service (MPS).

Find us at:

Facebook: Facebook.com/metpoliceuk

Twitter: @metpoliceuk
Appendix Two

Consent Form

Consent for Participation in Interview Research

I volunteer to participate in a research project conducted by Ms Ori Igwe from University of West London who is currently employed by the Crown Prosecution. I understand that the project is designed to gather academic information about international law enforcement cooperation and the prosecution of cyber stalkers. I will be one of approximately 30 people being interviewed for this research.

1. My participation in this project is voluntary. I understand that I will not be paid for my participation. I may withdraw and discontinue participation at any time without penalty. If I decline to participate or withdraw from the study, will be told.

2. I understand that most interviewees in will find the discussion interesting and thought-provoking. If, however, I feel uncomfortable in any way during the interview session, I have the right to decline to answer any question or to end the interview.

3. Participation involves being interviewed by academic researcher Ori Igwe. The interview will last approximately 30-45 minutes. Notes will be written during the interview. An audio tape of the interview and subsequent dialogue will be made. If I don't want to be taped, I will notify the researcher.

4. I understand that the researcher will not identify me by name in any reports using information obtained from this interview, and that my confidentiality as a participant in this study will remain secure. Subsequent uses of records and data will be subject to standard data use policies which protect the anonymity of individuals and institutions.
5. Colleagues will not be present at the interview or have access to raw notes or transcripts. This precaution will prevent my individual comments from having any negative repercussions.

6. I understand that this research study has been reviewed and approved by the research department of the London Metropolitan Force and the Crown Prosecution Service.

7. I have read and understand the explanation provided to me and I voluntarily agree to participate in this study.

8. I have been given a copy of this consent form.

____________________________ ________________________
My Signature                                                                 Date My Printed/Name

Signature of the Investigator   Ms Ori Igwe

For further information, please contact   Ori Igwe on 07971670497
Appendix Three

Interview Questions

Interviews with police officers

Question 1: Briefly outline your experience to date with law enforcement to do with cyber stalking?

Question 2: Have you received any training on cyber stalking?

Question 3: What is your definition of cyber stalking?

Question 4: What in your opinion are the issues with the definition of cyber stalking that needs to be addressed?

Question 5: What criminal category will cyber stalking be prosecuted under?

Question 6: What in your opinion is the threshold for distinguishing between rudeness, abuse and unpleasant comments on the internet and cyber stalking?

Question 7: What difficulties do the police face in the cross-jurisdictional investigation of cyber stalkers?

Question 8: As far as you are aware, what legislation do the police rely on to investigate cyber stalkers when it comes to cross jurisdictional cases?

Question 9: How effective do you think that the laws against cyber stalking are in the country?

Question 10: What are the existing extradition arrangements specifically relating to cyber stalking with:

(a) The US?
(b) The Republic of Ireland?

Question 11: To what extent from your experience do you think that the extradition arrangements are effective in the cross-jurisdictional investigation of cyber stalkers?

Question 12: What problems are you aware of that hinder the cross-jurisdictional investigation of cyber stalkers?

Question 13: What strategies are in place to combat cyber stalking and the illegal activities on the internet?

Question 14: Can you give examples of inter-jurisdictional co-operation with this kind of crime?

Question 15: What are the real practical difficulties with dealing with this type of crime?

**Interviews with prosecutors**

Question 1: Briefly outline your experience to date with law enforcement to do with cyber stalking?

Question 2: Have you received any training on cyber stalking?

Question 3: What is your definition of cyber stalking?

Question 4: What in your opinion are the issues with the definition of cyber stalking that needs to be addressed?

Question 5: What criminal category will cyber stalking be prosecuted under?
Question 6: What in your opinion is the threshold for distinguishing between rudeness, abuse and unpleasant comments on the internet and cyber stalking?

Question 7: What difficulties do the prosecutors face in the cross-jurisdictional investigation of cyber stalkers?

Question 8: As far as you are aware, what legislation do the police rely on to investigate cyber stalkers when it comes to cross-jurisdictional cases?

Question 9: How effective do you think that the laws against cyber stalking are in the country?

Question 10: What are the existing extradition arrangements specifically relating to cyber stalking with:

(a) The US

(b) The Republic of Ireland

Question 11: To what extent from your experience do you think that the extradition arrangements are effective in the cross-investigation of cyber stalkers?

Question 12: What problems are you aware of that hinder the cross-jurisdictional investigation of cyber stalkers?

Question 13: What strategies are in place to combat cyber stalking and the illegal activities on the internet?

Question 14: Can you give examples of inter-jurisdictional co-operation with this kind of crime?
Question 15: What are the real practical difficulties with dealing with this type of crime?

The interviews were conducted from four perspectives.
### Appendix 4

#### Total number of interviews

<table>
<thead>
<tr>
<th>Participants</th>
<th>Total number of Interviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police officers</td>
<td>25</td>
</tr>
<tr>
<td>Prosecutors</td>
<td>30</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>55</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Participants</th>
<th>Total number of Interviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member of parliament</td>
<td>1</td>
</tr>
<tr>
<td>Parliamentary research assistant</td>
<td>1</td>
</tr>
<tr>
<td>Probation official</td>
<td>1</td>
</tr>
<tr>
<td>Northern Ireland government adviser</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>4</strong></td>
</tr>
<tr>
<td>Participants</td>
<td>Total number of Interviews</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Assistant attorney general</td>
<td>1</td>
</tr>
<tr>
<td>Federal Secret Service Agent</td>
<td>1</td>
</tr>
<tr>
<td>Criminal Analyst</td>
<td>1</td>
</tr>
<tr>
<td>Executive and founder of a cyberstalking charity</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>4</td>
</tr>
</tbody>
</table>
**Interview Protocol**

**A The prosecutors' perspective**

The interviews provided an opportunity for prosecutors to give detailed accounts of the difficulties that they face in the prosecution of cross jurisdictional cyber stalkers. It also enabled the Prosecutors to identify the measures which in their opinions, need to be put in place to address the challenges that they face.

**B The police officers' perspective**

The interviews provided an opportunity for police officers to highlight the investigative hurdles that they face in trying to investigate cross-jurisdictional cyber stalkers. In doing so, the police officers identified measures which might facilitate international co-operation in the prosecution of cyber stalkers.

**C The government official's perspective**

The interviews afforded a member of parliament and a Northern Ireland government adviser the opportunity to confirm from the perspective of a government official, the steps that ought to be taken by the government to ensure that cyber stalking is criminalized in the UK.
D The probation officer's perspective

The interview enabled the former chair of the national probation office to identify from the perspective of victims, the problems that hinder the UK law enforcement officials from prosecuting cyber stalkers after the crime has been criminalized in the UK.
Appendix 5

STALKING ADVICE

Following the successful All Party Parliamentary Stalking Law Reform Inquiry, stalking became a criminal offence in 2012. 
**Stalking-Law-Reform-Findings-Report-2012**

Stalking is about fixation and obsession. It is a high risk factor for serious harm and homicide, as well as serious psychological harm if left unchecked. For this reason there are specific questions in the DASH about stalking and a subset of **12 Risk Screening Questions, S-DASH**.

(1) Stalking and harassment screening question (S-Dash)

**What if you are victim being stalking?**
If you have reported to the police and do not feel satisfied with their response, do not despair. If you answer positively to these questions, please take this checklist with you when you speak with the police and/or other agencies.

1. Are you very frightened?
2. Is there previous domestic abuse or stalking/harassment history?
3. Have they vandalised or destroyed your property?
4. Have they turned up unannounced more than three times a week?
5. Have they followed or loitered near your home or workplace?
6. Have they made threats of a physical or sexual violence nature?
7. Have they harassed or stalked any third party since the harassment began?
8. Have they acted violently towards anyone else during the stalking incident?
9. Have they engaged other people to help with their activities?
10. Has the stalker had problems in the past year with drugs, alcohol or mental health?
11. Is the stalker suicidal? Is there last resort thinking/finality?
12. Have they ever been in trouble with the police or do they have a criminal history?

For further specialist advice and support please call: Paladin, the National Stalking Advocacy Service 020 3866 4107

Link: [https://www.dashriskchecklist.co.uk/stalking-advice/](https://www.dashriskchecklist.co.uk/stalking-advice/)

[http://www.paladinservice.co.uk](http://www.paladinservice.co.uk)
(2) Stalking and Harassment Screening Questions (S-DASH)

S-Dash (2009) Risk identification checklist for use in stalking and harassment cases

Link:
https://www.reducingtherisk.org.uk/cms/sites/default/files/resources/risk/StalkingAndHarassmentS-DASH.pdf

(3) Joint NPCC and CPS Checklist – For Use by Police Forces and CPS in Cases of Harassment or Stalking

Date: Officer in case: 
Staff number: Case reference: 

The Police are to complete each box on the Checklist and send to the CPS in every case where charging advice or a charging decision is sought. The form is an important part of the evidential file - it should be fully and accurately completed. If the case also involves Domestic Abuse (DA) then the DA checklist should also be completed. This form does not replace the DA check list, but complements it.

Ensure that: timely decisions are made; a charging checklist is completed for each complainant (where more than one is involved); and the overall allegation is considered through the assessment of all available evidence, including the role and behaviour of the suspect.

The checklist does not replace the MG3, but should supplement it. The CPS should comprehensively endorse the MG3 including addressing any evidential weaknesses.

The safety of complainants, their friends, children and dependents is paramount. The risks to them must be carefully considered in these cases. Where possible, referrals to Independent Stalking Advocacy Caseworkers (ISACs), Independent Domestic Violence Advisors (IDVAs), or equivalent specialist service support should be made at the earliest possible opportunity.

The Police must refer to the College of Policing Authorised Professional Practice here.
Further information about charging cases of stalking or harassment is available here. Further information charging cases of domestic abuse cases is available here...
POLICE OFFICER - Before starting this checklist have you collected all available evidence, and have you given consideration to the wider pattern of behaviour, its cumulative impact and the context of the behaviour? Please ensure that all documentation referred to in the checklist is included with the file i.e. risk assessments, statements etc.

<table>
<thead>
<tr>
<th>YES</th>
<th>NO</th>
<th>COMMENT*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In cases of stalking, there is a pattern of unwanted, fixated and / or obsessive behaviour which is intrusive. It could be harassment that amounts to stalking or stalking that causes fear of violence or serious alarm or distress. Have you considered why this case does not meet the description of stalking?

YES | NO | COMMENT*
---|----|----------

Risk screening / risk assessment tool

101 / 999 Call

101 / 999 Call supplied to CPS Direct

Body Worn Video

Complainant’s statement - refer to all previous incidents if relevant and the impact the behaviour has had on the complainant)

Photographs; of tangible evidence such as damage and any injuries (taken over time as injuries develop). Photographs of perishable items i.e. flowers. Consider screenshots of text messages electronic communications etc. Consider CSI advice.

Admissions – especially were admissions are made about contact via social media.

Medical evidence / DNA (if available at the time); signed consent form; medical exhibits i.e. hair, presents

Other statements – children, attending officer, disposition of complainant/suspect, IDs of other persons present, and if relevant neighbours, family members, doctors, employers and work colleagues as well as specialist support services

Passive data/Comms data/Financial data e.g. data mining foot prints, social media/other electronic evidence, messages, diaries, spyware technology, apps, bank-records CCTV. Check all devices for incoming and outgoing data, WIFI and cell site data, including spyware (NB: communications data can be collected retrospectively from the service provide).

Relevant information to include from Police Records.

<table>
<thead>
<tr>
<th>YES</th>
<th>NO</th>
<th>COMMENT*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk of reoffending. Any previous risk screening / identification checklist with outcome

YES | NO | COMMENT*
---|----|----------

470
Any civil orders/proceedings and whether there has been previous breaches in any previous case (including DVPOs/DVPNs/PINs/court bail).

Any previous allegations (with URNs and including other complainants) and how these allegations were concluded (if case did not proceed why not?) DVDs.

Police to inform CPS of any breach or further offences, submit files to CPS and supply interview record in a timely way.

Were any firearms used? Does the suspect or members of the household have a firearms licence or are there any intelligence reports linking the suspect and/or household members to weapons?

<table>
<thead>
<tr>
<th>Information regarding the complainant and/or incidents.</th>
<th>YES</th>
<th>NO</th>
<th>COMMENT*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victim Personal Statement; if the complainant wishes to provide one (which should be updated throughout case proceedings and include the impact).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety of complainant (complainant’s views and specialist support service views if applicable).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whether complainant has been contacted by suspect/friends/family whether contact is supportive or intimidating – detail within comments section.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Counter allegations/defence.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information to support an application for bad character</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restraining Order – does the complainant want one and if so with what terms?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bail conditions that do not restrict the complainant and any children. Include locations to avoid.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Withdrawing support/retraction. There may be a number of reasons why the police might be asked not to proceed further including fear of further harm or repercussions. See CPS Legal Guidance for further information and steps to follow including the need for an officer’s statement on the appropriateness of a summons.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ability/willingness of complainant to attend court, give evidence and any special considerations.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Special measures needed? And type (views of complainant and specialist support service) need to complete an MG2.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The comment box must be completed if no evidence available or if the section is not applicable.
CPS Prompts for Prosecutors

Prosecutors must refer to the CPS Legal Guidance on Stalking and Harassment.

The table below provides some helpful prompts for prosecutors to consider and record in the MG3 and any case review.

<table>
<thead>
<tr>
<th>Provision and gathering of wider information in addition to this evidence gathering checklist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>If further evidence is required from the police ensure this is articulated in a clear and concise action plan, and discussed with the Officer as appropriate.</td>
</tr>
<tr>
<td>Find out whether there are any concurrent or imminent public law or private law family proceedings or civil proceedings and remedies involving the complainant or suspect.</td>
</tr>
</tbody>
</table>

**Assessing the suspect/defendant.**

Consider in every case of harassment that is referred through if this is a case of stalking?

Ensure timely applications for; admissions, hearsay evidence and/or bad character.

Has the credibility of the defendant been fully considered? E.g. Are there any previous instances of misconduct/convictions. Check CPS systems including CMS?

**Do any of the statutory defences apply?**

- Was the behaviour pursued for the purpose of preventing or detecting crime;
- Was it pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under any enactment; or
- In the particular circumstances of the case was the pursuit of the course of conduct reasonable?

Are there any other possible defences?

A plea to harassment in place of one of stalking should only occur on the rarest of occasions. When considering the acceptability of pleas has proper consideration been given to CPS Legal Guidance and the Attorney General’s Guidelines?

**Victim and witness support following a decision to charge.**

Victim Personal Statement obtained and updated throughout the case progression.

Timely consideration of; special measures, Pre-Trial Witness Interviews, expert evidence and other support measures.

Identification and consideration of vulnerabilities (BME, physical or mental impairment, LGBT, age).

On-going communication through Witness Care Units/other specialist services on case progression and any other useful information.

Where there is a withdrawal or retraction; see CPS Legal Guidance for further information on the possible reasons including fear or coercion, which should be fully explored with complainant/WCU/Specialist support.
## Appendix 6

### Codes

<table>
<thead>
<tr>
<th>Codes</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANON</td>
<td>Anonymous</td>
</tr>
<tr>
<td>CAOI</td>
<td>Cyberstalker’s awareness of impact</td>
</tr>
<tr>
<td>COM</td>
<td>Content of message</td>
</tr>
<tr>
<td>CP</td>
<td>Cultural Perception</td>
</tr>
<tr>
<td>CU</td>
<td>Central Unit</td>
</tr>
<tr>
<td>CSAMI</td>
<td>Cyberstalking and mental illness</td>
</tr>
<tr>
<td>CAW</td>
<td>Cannot access websites</td>
</tr>
<tr>
<td>CELVIC</td>
<td>Celebrity victims</td>
</tr>
<tr>
<td>CO</td>
<td>Claim ownership</td>
</tr>
<tr>
<td>CROSCOM</td>
<td>Cross Communicating</td>
</tr>
<tr>
<td>CUP</td>
<td>Cultural perception</td>
</tr>
<tr>
<td>CNAP</td>
<td>Cyberstalking not a priority</td>
</tr>
<tr>
<td>CVP</td>
<td>Cyberstalking via proxy</td>
</tr>
<tr>
<td>DEDLI</td>
<td>Deadline issues</td>
</tr>
<tr>
<td>DVI</td>
<td>Domestic violence issues</td>
</tr>
<tr>
<td>DL</td>
<td>Different laws</td>
</tr>
<tr>
<td>DEL</td>
<td>Delays</td>
</tr>
<tr>
<td>DISC</td>
<td>Discontinued cases</td>
</tr>
<tr>
<td>DOB</td>
<td>Duration of behaviour</td>
</tr>
<tr>
<td>DOC</td>
<td>Definition of cyberstalking</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ECC</td>
<td>Establishing course of conduct</td>
</tr>
<tr>
<td>EVID</td>
<td>Evidential difficulties</td>
</tr>
<tr>
<td>ELII</td>
<td>Existing laws ineffectively implemented</td>
</tr>
<tr>
<td>ECOD</td>
<td>Establishing a course of conduct</td>
</tr>
<tr>
<td>EXC</td>
<td>Excessive caseloads</td>
</tr>
<tr>
<td>FOC</td>
<td>Facts of case</td>
</tr>
<tr>
<td>FOR</td>
<td>Fear of repercussions</td>
</tr>
<tr>
<td>GOO</td>
<td>Gravity of offence</td>
</tr>
<tr>
<td>IOC</td>
<td>Intent of cyberstalker*</td>
</tr>
<tr>
<td>IOV</td>
<td>Impact on victims</td>
</tr>
<tr>
<td>INSE</td>
<td>Insufficient evidence</td>
</tr>
<tr>
<td>INS</td>
<td>Insufficient specialist</td>
</tr>
<tr>
<td>ISPI</td>
<td>Internet Service Providers issues</td>
</tr>
<tr>
<td>INSTFO</td>
<td>Insufficient time to follow up on initial reports</td>
</tr>
<tr>
<td>INTERM</td>
<td>Intermittent Relationships*</td>
</tr>
<tr>
<td>JURDI</td>
<td>Jurisdictional difficulties</td>
</tr>
<tr>
<td>LOA</td>
<td>Lack of awareness</td>
</tr>
<tr>
<td>LEG</td>
<td>Legislative difficulties</td>
</tr>
<tr>
<td>LENOT</td>
<td>Length of time</td>
</tr>
<tr>
<td>LD</td>
<td>Legislative difficulties</td>
</tr>
<tr>
<td>LOCD</td>
<td>Lack of centralized database</td>
</tr>
<tr>
<td>LOCU</td>
<td>Lack of centralized units</td>
</tr>
<tr>
<td>LOE</td>
<td>Lack of experts</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>LOFD</td>
<td>Lack of full disclosure</td>
</tr>
<tr>
<td>LOK</td>
<td>Lack of knowledge</td>
</tr>
<tr>
<td>LOR</td>
<td>Lack of resources</td>
</tr>
<tr>
<td>LOT</td>
<td>Lack of training</td>
</tr>
<tr>
<td>LOSU</td>
<td>Lack of separate units</td>
</tr>
<tr>
<td>LSL</td>
<td>Lenient sentencing laws</td>
</tr>
<tr>
<td>MOP</td>
<td>Missed opportunities</td>
</tr>
<tr>
<td>NAO</td>
<td>Not regulated</td>
</tr>
<tr>
<td>NOCD</td>
<td>Not obtaining charging decisions</td>
</tr>
<tr>
<td>NLRIISP</td>
<td>No laws requiring Internet Service Providers to assist</td>
</tr>
<tr>
<td>NOT</td>
<td>No training</td>
</tr>
<tr>
<td>NOSL</td>
<td>No single cyberstalking law</td>
</tr>
<tr>
<td>OEFDV</td>
<td>Obtaining evidence from domestic violence victims</td>
</tr>
<tr>
<td>OBT</td>
<td>Objective test</td>
</tr>
<tr>
<td>PCUP</td>
<td>Proving cases under S4A of the PHA</td>
</tr>
<tr>
<td>PGU</td>
<td>Poor global understanding</td>
</tr>
<tr>
<td>PNPOE</td>
<td>Police officers not providing outstanding evidence</td>
</tr>
<tr>
<td>PCPFE</td>
<td>Prosecutors chasing police officers for outstanding evidence</td>
</tr>
<tr>
<td>PMIC</td>
<td>Prosecuting mentally ill cyber stalkers</td>
</tr>
<tr>
<td>RAC</td>
<td>Risk assessment challenges</td>
</tr>
<tr>
<td>ROC</td>
<td>Risk assessment of cyberstalkers</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ROV</td>
<td>Risk assessment of victims</td>
</tr>
<tr>
<td>RSC</td>
<td>Registered sim cards</td>
</tr>
<tr>
<td>ROV</td>
<td>Reaction of victims</td>
</tr>
<tr>
<td>ROB</td>
<td>Restraining orders breached</td>
</tr>
<tr>
<td>RET</td>
<td>Red tape</td>
</tr>
<tr>
<td>STD</td>
<td>Statutory definition</td>
</tr>
<tr>
<td>SUBT</td>
<td>Subjective test</td>
</tr>
<tr>
<td>SOM</td>
<td>Shortage of manpower</td>
</tr>
<tr>
<td>SPOC</td>
<td>Single point of contact</td>
</tr>
<tr>
<td>STL</td>
<td>Statutory time limit for bringing offences</td>
</tr>
<tr>
<td>TOAB</td>
<td>Thresholds of acceptable online behaviour</td>
</tr>
<tr>
<td>USC</td>
<td>Unregistered sim cards</td>
</tr>
<tr>
<td>UNDR</td>
<td>Under reporting</td>
</tr>
<tr>
<td>UNPUB</td>
<td>Unrealistic public expectations</td>
</tr>
<tr>
<td>VIB</td>
<td>Victim behaviour*</td>
</tr>
<tr>
<td>VNSP</td>
<td>Victims not supporting prosecutions</td>
</tr>
<tr>
<td>VRTT</td>
<td>Victims refusing to testify</td>
</tr>
<tr>
<td>VWA</td>
<td>Victims withdrawing allegations</td>
</tr>
<tr>
<td>UNDR</td>
<td>Under reporting</td>
</tr>
<tr>
<td>VLOC</td>
<td>Victims lack of confidence in the police</td>
</tr>
<tr>
<td>VNRI</td>
<td>Victims not reporting incidents*</td>
</tr>
<tr>
<td>VOV</td>
<td>Vulnerability of victims*</td>
</tr>
<tr>
<td>VCC</td>
<td>Victims cross communicating*</td>
</tr>
<tr>
<td>VCRWC</td>
<td>Victims continuing relationships cyber stalkers*</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>VWI</td>
<td>Victims withholding information *</td>
</tr>
</tbody>
</table>

*Coding that emerged from the application of the Routine Activity Theory (Cohen and Felson, 1979) to the data*