Legality, Social Media and the Criminal Law

Laura Anne Higson-Bliss

Faculty of Arts and Science

This thesis is submitted to the Department of Law and Criminology, Edge Hill University, in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

September 2019

Abstract

Social media has changed how society communicates, transformed how individuals access the latest headline news and has altered many aspects of everyday life. It has, in turn changed the way in which individuals can target other members of society. In recent years, society has seen the likes of Facebook and Twitter used to distribute hate speech, accommodate revenge pornography and abuse others online. Consequently, the Government and the criminal justice system are being put under increasing pressure to tackle online abuse. Many of the current legal provisions contained in the law of England and Wales were enacted before the creation of social media. Yet these Acts are used to prosecute those who conduct abusive behaviour online. Issues are therefore arising with the adaptation of Acts of Parliament never intended to cover a digital age.

This thesis will critically examine several Acts of Parliament which have been used to control unlawful behaviour on social media sites, including, though not limited to, the Public Order Act 1986, the Malicious Communications Act 1988, and the Protection from Harassment Act 1997. It will be argued that the current use of these Acts breaches the fundamental principle of legality in the criminal law, before turning to examine freedom of speech and privacy online. Legality, at its very basic means the law needs to be accessible and clear to maintain the rule of law.

The final parts of this thesis will examine how other countries and institutions govern online behaviour. In the conclusive chapters, recommendations will be put forward as to how the legal system and society can better protect those who are abused online, including a draft social media Bill and a proposed universal code of conduct.

For my Dad, who is forever greatly missed.

Acknowledgments

I would firstly like to thank Edge Hill University and the Graduate Teaching scheme, without which, it is unlikely I would have been able to proceed with a PhD. In particular, my colleagues in the Department of Law and Criminology who have offered endless support and cups-of-tea when needed. I would also like to express my gratitude to my supervisors, Professor Francesco Rizzuto and Adam Pendlebury for their continued support throughout the completion of this thesis. Their endless encouragement has helped me achieve so much in my time at Edge Hill University.

To my friends who have always supported me, thank you for letting me vent! Without my girls, Kelly Wilson, Charna Hewitt, Jannette McMillian, Lauren Postlethwaite and Steph Farish, I would be lost. You have stood by me throughout the good and the bad. This PhD journey has not been easy and without the support of Grace Robinson, Sharon McAvoy, Kerry Richards and Julie Nightingale, I am not sure where I would be now. When everything felt so broken, your support helped pick me back up and see this through to the end; I am forever in your debt.

To my not so little brother James Bliss, thank you for always being there. I have often joked that most kids inherit money, instead, I inherited you, but I would not have it any other way. Lastly, I would like to thank my husband, Jonathan Higson-Bliss, for always being my shoulder to cry on, my ears to vent too and my celebration buddy!

However, the biggest thanks goes to my Dad, Colin Bliss; you are the reason I try so hard. Everything I do is to make you proud. I love and miss you more each day.

Table of Contents

Theoretical Positioning: Legality in the Criminal Law

Social Media Gatekeepers

Social Media, Criminal Law Regulation and Non-Technology-Based Legislation

Social Media, Criminal Law Regulation and Technology-Based Legislation: Part One

Social Media, Criminal Law Regulation and Technology-Based Legislation: Part Two

Freedom of Expression and Social Media

International Perspectives of Social Media and the Law

Recommendations

Table of Cases

Glimmerven en Hagenbeek v Netherlands [1979] ECTHR 8

Handyside v United Kingdom (1976)1 EHRR 737

Kafkaris v Cyprus App no 21906/04 (ECtHR, 12 February 2008)

Knuller (Publishing, Printing and Promotions) Ltd. and Others Appellants v Director of Public Prosecutions Respondent [1972] 3 W.L.R. 143, [1973] A.C. 435

Lau v Director of Public Prosecutions [2000] 1 F.L.R 799 (DC)

Majrowski v Guy's and St Thomas's NHS Trust [2005] EWCA Civ 251, [2005] Q.B 848

Majrowski v Guy's and St Thomas's NHS Trust [2006] UKHL 34, [2007] 1 A.C. 224

Pfeifer v Austria App no 125561/03 [2007] ECTHR 935

R v Abdul Sherif [2008] EWCA Crim 2653, [2009] 2 Cr. App. R. (S.) 33

R v Alison Chabloz Westminster Magistrates' Court 11 January 2018 (unreported)

R v Alison Chabloz Westminster Magistrates' Court 25 May 2018 (unreported)

R v Andrew Meldrum Woolwich Crown Court 30 May 2014 (unreported)

R v Blackshaw [2011] EWCA Crim 2312, [2012] 1 W.L.R. 1126

R v Chloe Cowan Canterbury Crown Court 14 July 2016 (unreported)

R v Clayton Kennedy Cardiff Magistrates Court 6 July 2015 (unreported)

R v Crosskey [2012] EWCA Crim 1645, [2013] 1 Cr. App. R. (S.) 76

R v Darryl O'Donnell Londonderry Magistrates Court 29 July 2011 (unreported)

R v David Jones Liverpool Magistrates 19 August 2015 (unreported)

R v Dooley (Michael) [2005] EWCA Crim 3093, [2006] 1 W.L.R. 775

R v Edward Leonard Hall (1985) 81 Cr. App. R. 260

R v G and Another [2003] UKHL 50, [2004] 1 A.C. 1034

R v Gold (Steven William), Schifreen (Robert Jonathan) [1988] A.C. 1063

R v Jason Asagba Reading Magistrates' Court 1 September 2015 (unreported)

R v Jordan Blackshaw Chester Crown Court 16 August 2011 (unreported)

R V Liam Stacey Swansea Crown Court On Appeal From The Magistrates' Court A20120033.

R v Martin Hartshorn Grimsby Crown Court 4 November 2011 (unreported)

R v Matthew Woods, Chorley Magistrates Court, 8 October 2012 (unreported)

R v Paul Chambers, Doncaster Magistrates' Court, 10 May 2010 (unreported)

R v Perry Sutcliffe-Keenan Chester Crown Court 16 August 2011 (unreported)

R v Peter Nunn The City of London Magistrates Court 29 September 2014 (unreported)

R v Rhodri Phillips Westminster Magistrates' Court 13 July 2017 (unreported)

R v Rimmington, R v Goldstein [2005] UKHL 63, [2006] 1 A.C. 459

R v Sadique and Hussain (No2) [2013] EWCA Crim 1150, [2013] 2 Cr. App. R. 31

R v Sean Duffy Reading Magistrates' Court 13 September 2011 (unreported)

R v Sheppard and Whittle [2010] EWCA Crim 65

R v Smith (Gavin) [2012] EWCA Crim 398, [2012] 1 W.L.R. 3368

Regina Respondent v Ireland Appellant [1997] 3 W.L.R. 534, [1998] A.C. 147

Regina Respondent v Woollin Appellant [1998] 3 W.L.R. 382, [1999] 1 A.C. 82

S v Crown Prosecution Service [2008] EWHC 438

Shreya Singhal v Union of India (2013) 12 S.C.C. 73

Southard v Director of Public Prosecutions [2006] EWHC 3349 (Admin), [2007] A.C.D. 53

Stoker v Stoker [2019] UKSC 17

Sunday Times v United Kingdom (1979) 2 EHRR 245

SW v United Kingdom, CR v United Kingdom App no 20166/92 (ECtHR, 22 November 1995)

Sweet v Parsley [1969] 2 W.L.R. 470, [1970] A.C. 132

Taylor's Central Garages (Exeter) v Roper [1951] 2 T.L.R. 284

Welch v United Kingdom App no 17440/90 (ECtHR, 9 February 1995)

Yildirim v Turkey App no 3111/10 ECTHR 2012-VI

Table of Legislation

Public Order Act 1936

Public Order Act 1986

Serious Crime Act 2007

Serious Crime Act 2015

Serious Organised Crime and Police Act 2005

Sexual Offences (Amendment) Act 1992

Sexual Offences Act 2003

Sporting Events (Control of Alcohol ect) Act 1985

Summary Offences Act 1966

Telecommunications Act 1984

European Legislation, Conventions, Treaties and Directives

European Convention on Human Rights and Fundamental Freedoms

Universal Declaration of Human Rights

International Covenant on Civil and Political Rights

Consolidated versions of the Treaty of European Union and the Treaty on the Functioning of the European Union [2016] C 202/01

Treaty of Lisbon [2007] OJ C-306/1

The Treaty of Rome [1957]

Directive on Copyright in the Digital Single Market 2016/0280

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000

Australia

Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019

Enhancing Online Safety Act 2015

Summary Offences Act 1966

Criminal Code Act (1995)

Germany

Act to Improve Enforcement of the Law in Social Networks (2017)

German Criminal Code (Strafgesetzbuch)

India

Information Technology Act 2000

Indian Penal Code

Table of Figures

Research Questions

1. To what extent does the criminal justice system, social networking companies and society govern online abuse aided by social media?

2. How does the current criminal law of England and Wales prohibit online abuse?

3. To what extent can other international approaches to online abuse aid how the criminal justice system in England and Wales tackles social media abuse?

4. How can the criminal justice system, social networking companies and society better protect those who are subjected to abusive conduct on social media?

Introduction

> '[T]he Internet provides a forum for the dissemination of potentially harmful false information to huge audiences. This might mean that certain behaviour which has been tolerated offline now arguably warrants criminal sanction, at least in online contexts.'[1]

Many of the harms associated with the Internet are not unique to the digital age, in fact, they have always existed within society but now occur more openly. The Internet dominates much of society today. In the United Kingdom alone 90% of adults are regular users of the Internet.[2] It has changed many aspects of everyday life, from how we obtain our news, to how we communicate with others. The Internet can be both a force for good and a force for bad, this is particularly true when examining the use of social media in a digital age.

Though there is no true definition of social media, as discussed in detail in the following chapter it has become prevalent within a digital society. In essence, social media allows users to instantly communicate with others online, build online profiles, and share information with others at the click of a button. It has changed many aspects of the physical world such as campaigning, which can now be aided or solely run online. For example, campaigns have emerged online tackling the subtle everyday sexism that still

[1] Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018) [11.122]
[2] Office of National Statistics, 'Internet users, UK: 2018' (*Office of National Statistics*, 31 May 2018) <https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2018> accessed 2 November 2018

exists within society,[3] campaigns to highlight sexual harassment,[4] and campaigns to tackle the stigma surrounding domestic violence.[5] Yet as will be discussed throughout this thesis there is a darker side to social media, in which bullying, harassment and trolling are flourishing online.

The use of social media to torment others online, commonly referred to as online abuse, is a prevalent problem within society today. Research, as discussed in chapter one, has started to emerge exposing both the extent of online abuse and the consequences this behaviour can have upon the victim. Its effects have included withdrawal from social life,[6] changes in a person's online presence,[7] and significant mental health issues, including post-traumatic stress disorder,[8] self-harm,[9] and suicide.[10] However, as discussed in detail in the following chapter, like that of social media, there is no true definition of abuse, which can lead to inadequacies in the current literature

[3] Laura Bates, 'The everyday sexism project' (*Everydaysexism*, 2019) <https://everydaysexism.com/> accessed 6 February 2019
[4] Bri Lee, 'Sharing our stories is the strength at the heart of #MeToo. We must repeal gag laws' *The Guardian* (London, 19 November 2018) <https://www.theguardian.com/commentisfree/2018/nov/19/sharing-our-stories-is-the-strength-at-the-heart-of-metoo-we-must-repeal-gag-laws> accessed 27 November 2018
[5] Jessamy Gleeson, '"(Not) working 9–5": the consequences of contemporary Australian-based online feminist campaigns as digital labour' (2016) 16(1) Media International Australia 77 <http://journals.sagepub.com/doi/pdf/10.1177/1329878X16664999>
[6] Mudasir Kamal & William J. Newman, 'Revenge Pornography: Mental Health Implications and Related Legislation' (2016) 44(3) American Academy of Psychiatry and the Law 359, 362
[7] Committee on Standards in Public Life, *Intimidation in Public Life: A Review by the Committee on Standards in Public Life* (HC 2017-18) 39
[8] Samantha Bates, '"Stripped": An Analysis of Revenge Porn Victims' Lives after Victimization' (Master of Arts Thesis, Simon Fraser University 2015) 24
[9] Ann John *et al*, 'Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review' (2018) 20 (4) Journal of Medical Internet Research 129
[10] Sarah Knapton, 'Cyberbullying makes young people twice as likely to self harm or attempt suicide' *The Telegraph* (London, 22 April 2018) <https://www.telegraph.co.uk/science/2018/04/22/cyberbullying-makes-young-people-twice-likely-self-harm-attempt/> accessed 4 October 2018

on online abuse. For the purpose of this thesis and as will be justified in the following chapter, abuse is defined as:

> Insulting and hostile behaviour aimed at another online which causes the deterioration of another's physical and mental wellbeing; threats of physical and/or sexual violence; insulting and hostile behaviour aimed at another because of their (if real or presumed) gender, race, ethnicity, religion, national origin, gender identity, sex, disability or sexual orientation.

Consequently, abuse is given a subjective meaning, in which the terms such as inappropriate, unlawful, and harmful are used interchangeably. It is acknowledged that conduct which can be labelled as harmful is not always illegal, however, the distinction is not always easy to find; as will be illustrated throughout this thesis. Despite issues with definitions increasing pressure has been placed on the criminal justice system, the Government and social media companies to do more in helping to reduce online abuse.

In 2013 following a number of high-profile cases[11] relating to inappropriate behaviour online, the Crown Prosecution Service (CPS)[12] produced their first prosecuting guidelines on communications sent *via* social media (the guidelines).[13] The guidelines were produced following growing concerns about the lack of consistency with the prosecution of social media offences across England and Wales. Yet since the implementation of the guidelines prosecutions for social media related offences have been on the decline,[14]

[11] For instance, *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin), [2013] 1 WLR 183
[12] The role of the CPS will be discussed in detail in chapter two.
[13] The Crown Prosecution Service, 'Guidelines on Prosecuting Cases Involving Communications Sent via Social Media' (*CPS.gov*, 2016) <http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/> accessed 10 October 2016
[14] Ministry of Justice, 'Criminal Justice System statistics quarterly: December 2017' (*Gov.uk*, 17 May 2018) <https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2017> accessed 25 February 2019

despite increasing reports being made to the police.[15] In 2017 research undertaken by the BBC exposed a dramatic increase in reports being made to police forces across England and Wales, concerning malicious communications online.[16] The BBC uncovered that between 2015 and 2016 there had been an increase of 36,462 police reports involving malicious communications,[17] placing significant pressure on police forces across England and Wales.

Arguments have therefore started to emerge suggesting that the criminal justice system is not keeping pace with changing technology,[18] resulting in several Government and parliamentary investigations. In April 2019 the Government released its first White Paper concerning online harms.[19] The arguments put forward in the White Paper, which are considered 'ambitious',[20] focus on holding social media companies to account for inappropriate behaviours which continue to be a problem across their sites. Whereas this thesis will focus on a multidimensional approach.

Methods and Methodology

The purpose of this thesis is to examine how the criminal justice system of England and Wales, social networks and society can better aid those

[15] The BBC, 'Teenager's life "ruined" by Live.me and Twitter "trolls"' *The BBC* (London, 24 October 2017) <http://www.bbc.co.uk/news/uk-england-41693437> accessed 30 January 2018
[16] *Ibid.,*
[17] *Ibid.,*
[18] Communications Committee, *Regulating in a digital world* (HL 2017-19, 299) 3
[19] HM Government, *Online Harms White Paper* (CP 57, 2019)
[20] *Ibid.,* 1

subjected to online abuse. To do this, a narrative review of Acts governing unlawful social media usage will be deconstructed, keeping into account the Acts historical and social background, discussed in detail below. This is a similar approach undertaken by Scaife,[21] who uses a narrative review of the literature to demonstrate to the reader how both the civil and criminal law applies in a social media context. However, this thesis constructs a narrative review through the lens of legality. Legality, which underpins the theoretical perspective of this thesis, is the principle that the law needs to be in place, clear and certain in order for individuals to conform to it.[22] For an in-depth discussion on legality and why other theoretical approaches were disregarded, see chapter two.

At its very basic, a narrative review is a comprehensive and critical analysis of the current knowledge on a given topic.[23] In this case, journal articles, books, research studies, case law examples, legal discourse, newspaper articles and Acts of Parliament will be scrutinised, to truly understand the application of the criminal law in a social media context. This allows for an in-depth analysis to take place of the current criminal law framework in England and Wales and its application in a social media scenario. The benefits of conducting a narrative review of the literature throughout this thesis allow for the researcher to present a variety of up-to-date studies related to social media abuse, as opposed to focussing on primary research conducted purely

[21] Laura Scaife, *Handbook of Social Media and the Law* (Routledge 2015)
[22] Article 7 of the European Convention on Human Rights and Fundamental Freedoms
[23] Rumona Dickson, M. Gemma Cherry and Angela Boland, 'Carrying Out a Systematic Review as a Master's Thesis' in Angela Boland, M. Gemma Cherry & Rumona Dickson (eds) *Doing a Systematic Review: A student's Guide* (2nd edn, Sage 2014) 11-12

for this study. This allows for a critical analysis of the current social media narrative to take place across the thesis as opposed to one separate literature review chapter. Whilst other methods could be utilised, such as interviews or questionnaires, due to ethical constraints and issues in getting participants to take part in the research, it was decided that a narrative review was more appropriate for the research questions posed.

The Acts and legal discourse reviewed throughout this thesis have been chosen through an analysis of the wider literature, in particular the work of Scaife.[24] As the focus of this thesis is on the criminal law, civil provisions which can be used to govern online conduct, for example defamation, have been disregarded as it was beyond the scope and purpose of the research questions. There are however other criminal law provisions[25] which can be used in a social media context which are not discussed in the thesis; because of all the Acts used to control online behaviour, the Acts reviewed in the following discussions give rise to the most significant arguments that the law does not comply with the principle of legality.

Throughout the following discussions, a non-consequentialist approach will be used, whereby the researcher is interested in the process undertaken by the criminal justice system in determining why a particular Act of Parliament is utilised in a given situation. For example, why the Serious Crime Act 2007

[24] Scaife n.21
[25] For example, Section 16 Offences Against the Person Act 1861 which prohibits threats to kill

was used in the case of *R v Blackshaw*,[26] but not in *R v Rhodri Phillips*,[27] as discussed further in chapter four. Due to the way in which the criminal justice system works in England and Wales, the cases reviewed in the following chapters have been chosen as they have either been officially recorded and published, or significant case facts were published by the media and therefore sufficient information about the cases are in the public domain. The following discussions will centre on the concept that the current criminal law framework when applied in a social media setting, does not conform to the principle of legality, discussed further in chapter two. Consequently, it is argued that the current criminal law framework, in a social media context, is being either misunderstood by actors in the criminal justice system or indeed being used in an arbitrary manner.

Using a non-consequentialist approach through the lens of legality, the findings will be presented in a systematic manner, allowing for further discussions to take place as to how actors in the criminal justice system, i.e the police and the CPS, social networking companies and society can better protect those subjected to online abuse. This will be aided further by the narrative review of the current social media literature examined throughout varies points of this thesis. In addition, to enhance the recommendations put forward in chapter nine, an examination of how the European Union, Australia, Germany and India have attempted to govern online conduct will occur in chapter eight. The primary reason for focussing on these four

[26] *R v Blackshaw* [2011] EWCA Crim 2312, [2012] 1 W.L.R. 1126
[27] *R v Rhodri Phillips* Westminster Magistrates' Court 13 July 2017 (unreported)

institutions and countries relates to the unique approach each has taken in attempting to tackle online abuse.

Research Questions

Using a narrative review of the literature from the theoretical perspective of legality, the following research questions will be answered:

1. To what extent does the criminal justice system, social networking companies and society govern online abuse aided by social media?

2. How does the current criminal law of England and Wales prohibit online abuse?

3. To what extent can other international approaches to online abuse aid how the criminal justice system in England and Wales tackles social media abuse?

4. How can the criminal justice system, social networking companies and society better protect those who are subjected to abusive conduct on social media?

Chapter Overview

Chapter one provides a contextualisation of the underlying theme of this thesis, online abuse. It takes the format of exploring the dominance of the Internet within society today. Using the work of Bernal, the purpose of the

Internet will be examined,[28] before turning to look at social media. As highlighted above there is no one true definition of social media, but as will be explained in the contextualisation chapter, for the purpose of this thesis social media is defined as:

> 'the ability to share, to co-operate, with one another, and to take collective actions, all outside the framework of traditional institutions and organisations.'[29]

Though it is estimated that there are over 200 social media companies across the globe,[30] as explained in chapter one, this thesis will focus on two of the biggest social media companies today, Facebook and Twitter. Their sheer dominance will be detailed in the contextualisation chapter. The final section of chapter one will provide a comprehensive discussion of the extent of online abuse today, providing the rationale as to why it is important that the law adequately protects individuals from online abuse.

Chapter two will give a brief overview of the criminal justice system in England and Wales, before going on to justify why the theoretical position of legality was used to underpin key arguments in this thesis. To do this, other theoretical concepts, in particular deterrence theory, rational choice theory, feminism, digital feminism and victimology will be discussed first before turning to examine legality, allowing the researcher to justify their theoretical positioning. Legality consists of three interlinking rules: the law must be in place, the law must be clear, and the law must be accessible. Though

[28] Paul Bernal, *The Internet, Warts and All: Free Speech, Privacy and Truth* (Cambridge University Press 2018) 5-19
[29] Clay Shirky, *Here comes everyone* (Penguin 2008) 20. For a discussion on different definitions of social media see, Christian Fuchs, *Social Media a Critical Introduction* (Sage Publications 2014) 35-37
[30] Scaife n.21, 4

elements of other theories, such as those listed above, are present at varies points of this thesis, it will be argued that the concept of legality underpins the criminal law; failure to abide by this principle can cause misunderstandings, leaving victims of online abuse frustrated, alongside raising issues with the law being used in an arbitrary manner.

Following growing concerns about the extent of online abuse, social media companies have been put under increasing pressure to do more to control inappropriate behaviours on their sites.[31] Chapter three examines in detail how both Facebook and Twitter are currently trying to tackle online abuse. The chapter starts by outlining both Facebook and Twitter's terms of service agreements, before turning to look at the different mechanisms each company has put in place to make their sites safer for online users. Chapter three will conclude by suggesting that self-regulation is currently failing to adequately protect users from online abuse, providing the reasoning as to why the law needs to intervene.

To determine how the current criminal law framework of England and Wales governs online abuse aided by social media, chapter's four to six examine several legislative provisions which have been applied in cases relating to online abuse. Chapter four examines in detail legislative provisions which are currently being utilised in a social media context, which were never intended to cover technology. Each Act, the Serious Crime Act 2007, the Public Order Act 1986 and the Protection from Harassment Act 1997, are taken in turn

[31] See, Communications Committee n.18

and critically analysed from a social media perspective. Here, the purpose behind the creation and implementation of each Act will be stated, before turning to look at both the *actus reus* and *mens rea* of the behaviours prohibited under these Acts of Parliament.[32] It will be put forward in this chapter that each of these Acts does not comply with the principle of legality in the criminal law. It will conclude by suggesting a number of recommendations to better govern inappropriate conduct carried out online.

Following on from examining non-technology-based Acts of Parliament, chapter five discusses both the Computer Misuse Act 1990 and section 33 of the Criminal Justice and Courts Act 2015. Both these provisions were implemented to cover new technology, though it is unlikely that the Computer Misuse Act was created with social media in mind. Chapter five argues that both these Acts conform to the principle of legality in the criminal law, and therefore need to be utilised to better protect individuals from online abuse. However, chapter five does highlight issues with how section 33 of the Criminal Justice and Courts Act is constructed. Section 33 of the Criminal Justice and Courts Act prohibits revenge pornography. Revenge porn is:

> 'the sharing of private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress.'[33]

The law prohibiting revenge porn has been constructed in a narrow manner. For instance, as discussed in chapter five a person who sends revenge porn images will only be found guilty if it can be established that they sent the

[32] The meaning of *actus reus* and *mens rea* will be explained in chapter two.
[33] HM Government, 'Revenge Porn: The Facts' (*Gov.uk*, 2014) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/405286/revenge-porn-factsheet.pdf> accessed 19 October 2016

image or video in question to cause distress. Consequently, images or videos sent for other reasons, for example for financial gain, are outside the realms of the Act.

Whereas both the Computer Misuse Act and section 33 of the Criminal Justice and Courts Act govern specific conduct carried out online, the Malicious Communications Act 1988 and section 127 of the Communications Act 2003 can be considered as covering miscellaneous online offences. Both these provisions as highlighted in chapter six can be seen to have taken precedence in a social media context. Indeed, as argued by Scaife both Acts have become interchangeable in recent years.[34] Issues have therefore arisen throughout the criminal justice system regarding the use of the Malicious Communications Act and section 127 of the Communications Act to govern inappropriate behaviours online. Chapter six examines in detail these two Acts of Parliament, looking at both the *actus reus* and *mens rea* of the offences prohibited under both provisions. Here, it is argued that the current use of the terms 'menacing', 'indecent' and 'grossly offensive' material, does not comply with the principle of legality, using case examples to illustrate these points. The final part of this chapter will critically analyse the current social media prosecuting guidelines implemented by the CPS in 2013, before making a number of recommendations. The discussions throughout chapters two, three, four, five and six will answer research questions one and two.

[34] Scaife n.21, 166

Moving on from critically analysing the current criminal law framework in England and Wales, chapter seven examines freedom of expression and the right to privacy, as protected under the European Convention on Human Rights and Fundamental Freedoms. These two competing rights are not unique to the digital age, they have always existed with traditional types of media. However, as explored in chapter seven freedom of expression has become somewhat the trump card in cases relating to online conduct. Here, it is argued that the criminal justice system currently tilts in the direction of freedom of expression. This chapter concludes by suggesting that privacy, which includes a person's right to physical and psychological integrity, should be considered in the first instance, before turning to examine freedom of expression.

In order to answer the third research question chapter eight explores how the European Union, Australia, Germany and India are currently attempting to tackle inappropriate behaviours online. The rationale for focussing on these institutions and countries relates to the different approaches each has taken to controlling online abuse. Both the European Union and Australia endorse non-legislative approaches to governing online conduct. Whereas Germany has implemented the Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) 2017, which is directly aimed at social media companies to do more in removing unlawful content from their sites. In contrast, India has implemented a specific legal provision directly aimed at the online user. The chapter concludes by suggesting that a mixed-method

approach is needed to adequately protect victims from online abuse.

The final research question poses to discuss alternative ways in which the criminal justice system and society can better protect those subjected to online abuse. Using the arguments put forward in the previous chapters, chapter nine suggests several recommendations to help tackle the growing issue of online abuse. It is argued in chapter nine that a multidimensional approach is needed to keep pace with changing technology whereby we need changes within the law, the criminal justice system as a whole, education and society in order to better protect those subjected to abusive behaviour online.

Contribution to knowledge

This project makes the following original contributions to knowledge; it will consist of:

1. A critical evaluation of the law's response to online abuse from the perspective of legality;
2. To put forward several recommendations to help combat the growing issue of online abuse, taking into consideration international approaches to tackling abuse online;
3. A proposed social media Bill to better protect individuals from online abuse.

Chapter One

Contextualisation: The Internet and Online Abuse

> 'So, the Internet is an information resource, a communications medium, a business platform, a political platform and a public space - and all at the same time, using the same services and systems, even within the same conversations and interactions. It is where people converse and socialise, where they organise their "offline" lives, where they find jobs and romance, where they shop, where they find entertainment.'[1]

The Internet has altered and shaped society since the 1960s. It has changed how society communicates, shops and socialises, in fact the Internet dominates much of society today. In that most prevalent of roles, it has become '… both a nuisance and a positive thing'.[2] The following discussion will outline the history of the Internet, looking particularly at the emergence of Web 1.0 and Web 2.0. Here, emphasis will be placed on the purpose behind its creation, before moving on to examine in detail the use of the Internet as a new form of instant communication and the development of social media. The final parts of this chapter will expose the ongoing issue of social media sites being used as a weapon to torment and abuse others online. Before turning to look at the creation of the Internet, a brief overview will be given of the criminal justice system in England and Wales.

The Internet: A brief history

There is no true definition of what constitutes the Internet, though there is a consensus of certain characteristics which can be associated with it:

> 'The Internet is a framework that allows users to exchange information at a distance, work, carryout research, discuss, transfer files as well

[1] Paul Bernal, *The Internet, Warts and All: Free Speech, Privacy and Truth* (Cambridge University Press 2018) 19
[2] Ursula Smartt, *Media & Entertainment Law* (Taylor & Francis 2017) 72

as a range of other activities.'[3]

In essence, the Internet 'is basically a telecommunications system for computer networks'[4] with its origins stemming back to the 1960s.

In October 1957 Western society was taken by surprise at the announcement that the Soviet Union had launched the first man-made object into outer space.[5] Following this, the then President of the United States of America Dwight Eisenhower, created a new research agency, the Advanced Research Projects Agency, linked to the Department of Defence. The purpose of the agency was to ensure the USA would never again be taken by surprise at the emergence of new technology.[6] The Advanced Research Projects Agency created the world's first successful computer network, known as the ARPANET (the Advanced Research Projects Agency Network) in the late 1960s.[7]

Following the success of ARPANET, further networks were manufactured including the Transmission Control Protocol, which allowed networks to be created between local computers.[8] In 1988 computers based in Canada and France were linked to networks created in the United States, paving the way for the creation of the World Wide Web.[9]

---

[3] Kevin M Rogers, *The Internet and the Law* (Macmillan International Higher Education 2011) 3
[4] Andrew Murray, *Information Technology Law: The Law and Society* (3rd edn, Oxford University Press 2016) 16
[5] *Ibid.,*19
[6] *Ibid.,*17
[7] *Ibid.,* 20
[8] Jeffrey C Jackson, *Web Technologies: A Computer Science Perspective* (Pearson Education 2007) 2
[9] *Ibid.,* 3

The World Wide Web consists of millions of interlinked web pages which use the Internet to connect. The foundation for the World Wide Web was created in 1989 by Sir Tim Berners-Lee.[10] Berners-Lee envisioned a database where users would be able to obtain any information they desired with minimum fuss. In 1990 the first website went 'live'.[11] By 1993 the World Wide Web or Web 1.0 as it is commonly referred to, was made available to the wider public. The purpose of Web 1.0 was to allow users to actively search between static websites.[12] In essence, Web 1.0 was an information database, whereby users were considered as consumers.[13]

By the turn of the next millennium, the advancement of changing technology had altered Web 1.0 completely. Internet users went from consumers to content creators.[14] By 2005 it had been accepted that a new version of the World Wide Web had been created, Web 2.0:

> 'The term Web 2.0 … is said to describe the period in which websites became more interactive, collaborative, and social. This is typically contrasted with more passive website interactions, where users simply viewed or downloaded content from websites.'[15]

Web 2.0 unlike its predecessor, was much more interactive, dynamic and user-driven.[16] The expansion of the World Wide Web changed the job

---

[10] Rogers n.3, 3
[11] Madhumita Murgia, 'The world's first website went online 25 years ago today' *The Telegraph* (London, 21 December 2015) <https://www.telegraph.co.uk/technology/internet/12061803/The-worlds-first-website-went-online-25-years-ago-today.html> accessed 2 November 2018
[12] Rogers n.3, 213
[13] Matthew Allen, 'What was Web 2.0? Versions as the dominant mode of internet history' (2012) 15(2) New Media & Society 260, 263
[14] *Ibid.,*
[15] Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018) [2.29]
[16] Rogers n.3, 213

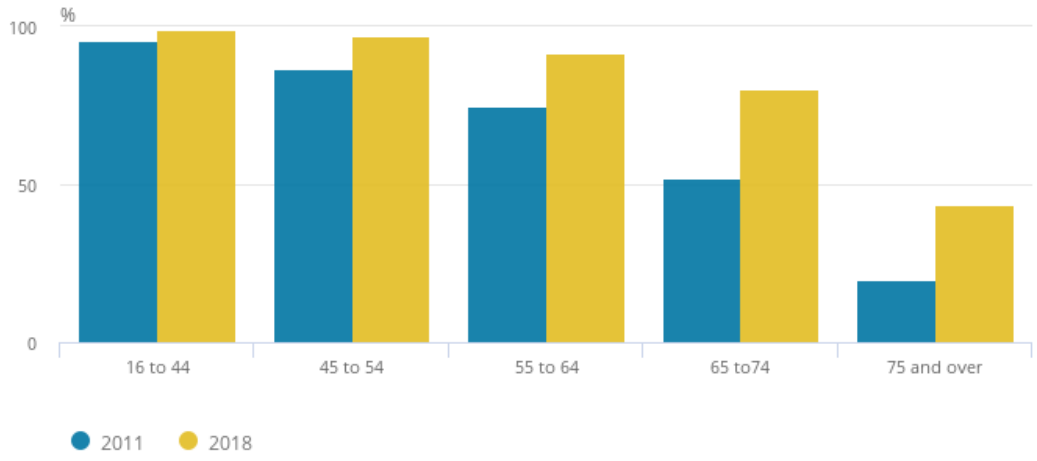
market, altered how individuals communicated, and has become integral to the way in which society functions.

Internet Growth and Usage

Since its creation in 1989 the World Wide Web and the Internet has grown in terms of websites and online users.[17] In the United Kingdom by 2018, 90% of adults were regular Internet users, an increase of 1% on the previous year. Of those aged between 16 and 34, 99% were regular users of the Internet, demonstrated further in figure one.[18] Similarly, Internet usage has increased across the world. In 2017 it was reported that 3.58 billion people worldwide were users of the Internet, an increase of 190 million on the previous year.[19] With the expansion of Internet usage, the purpose for which it was designed has adapted to the changing needs of society. The World Wide Web has gone from static websites, whereby users were able to use the Internet as an information database, to interactive websites, which allow for instant communication, political debate and the selling of goods online.[20]

[17] Internet websites have since expanded from 130 in 1993 to 17,087,182 by the end of 2000. See, Internet Live Stats, 'Total number of Websites' (*Internet Live Stats*, 2018) <http://www.internetlivestats.com/total-number-of-websites/> accessed 2 November 2018
[18] Office of National Statistics, 'Internet users, UK: 2018' (*Office of National Statistics*, 31 May 2018) <https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2018> accessed 2 November 2018
[19] Statista, 'Number of Internet users worldwide from 2005 to 2017 (in millions)' (*Statista*, 2018) <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/> accessed 2 November 2018
[20] Note, this is not a definitive list.

Figure 1: *Recent Internet usage by age, 2011 and 2018, UK.*[21]



Source: Office for National Statistics

Furthermore, access to the online world has moved away from dial-up connections[22] on processing computers to easy access *via* smartphone technology.[23] Consequently, the purpose of the Internet has expanded, as illustrated in the work of Bernal. Bernal suggests that the purpose of the Internet can be split into six categories: the use of the Internet as an information database, the use of the Internet as a business platform,[24] the use of the Internet as a political platform, the Internet as a public space, the Internet as a communications device, and the use of the Internet in being integral to society.[25]

[21] Office of National Statistics n.18
[22] Dial-up refers to 'the method for connecting to an IPS using a regular telephone line …'. See, Gary B Shelly & Jennifer Campbell, *Discovering the Internet: Brief* (Cengage Learning 2011) 19
[23] On average in the United Kingdom smartphone users spent 2 hours per day on the internet using their mobile phones. See, Ofcom, 'The UK is now a smartphone society' (*Ofcom*, 6 August 2015) <https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2015/cmr-uk-2015> accessed 30 November 2018
[24] The use of the Internet as a business platform will not be discussed as it is beyond the scope of this thesis.
[25] Bernal n.1, 5-19

The Internet as an Information Database

The original purpose of Web 1.0 was to create an information database where users could easily access information from a computer. The concept of the World Wide Web as an information database has since expanded; users can now actively search for information, access the latest headline news,[26] and keep updated with the latest celebrity gossip.

Information obtained from the Internet is usually gathered *via* search engines such as Google. Google dominates much of the search engine market around the world.[27] Encyclopaedias, which were once only obtainable in hard copy, are now readily available online. For instance, Wikipedia an online encyclopaedia, has over 43 million pages covering a range of topics.[28] Yet the use of the Internet as a form of imparting information has raised issues concerning the validity of the information imparted.

The United Kingdom European Union membership referendum (Brexit)[29] in 2016, and the 2017 General Election in the United Kingdom, along with the Presidential campaign in the United States of America in 2016/17, exposed growing concerns about the validity of information obtained from the

[26] Research undertaken by Ofcom in 2016 exposed that 48% of adults now use the Internet for news. See, Ofcom, 'News consumption in the UK: 2016' (*Ofcom*, 29 June 2017) 34 <https://www.ofcom.org.uk/__data/assets/pdf_file/0016/103570/news-consumption-uk-2016.pdf> accessed 14 November 2018

[27] Bernal n.1, 5

[28] *Ibid.,*

[29] In 2016, the citizens of the United Kingdom voted in favour of leaving the European Union following a referendum. The departure of the United Kingdom from the European Union is commonly referred to as Brexit.

Internet.[30] These key political moments were dominated by fake news and data harvesting.[31] Fake news can be defined as 'purposefully false and provocative misinformation and literally untrue news stories.'[32] During these political events in the United Kingdom and the United States of America, fake news dominated the Internet. For instance, Facebook, the world's largest social media company,[33] has made available to an inquiry examining the extent of fake news during the Brexit referendum, advertisements and stories that were actively shared across their site which were false.[34] For example, one article which was actively shared across Facebook stated that the European Union (EU) blocks citizens ability to speak out and protect polar bears,[35] a story which was later proven to be false.[36] Fake news articles were therefore being used to target voters, which became more apparent in the wake of the Cambridge Analytica Scandal in 2018.

[30] Digital, Culture, Media & Sport Committee, *Disinformation and "fake news": Interim Report* (HC 2017-179 363)
[31] 'Harvesting data, as its agricultural name suggests, is similar to gathering crops because it involves collection and storage with the expectation of future reward.' See, Gráinne Maedhbh Nic Lochlainn, 'Facebook data harvesting: what you need to know' *The Conversation* (London, 3 April 2018) <http://theconversation.com/facebook-data-harvesting-what-you-need-to-know-93959> accessed 5 February 2019
[32] Rob William, 'Fighting "Fake News" in the Age of Digital Disorientation: Towards "Real News" Critical Media Literacy Education, and Independent Journalism for 21st Century Citizens' in Christian Z Goering & Paul L Thomas (eds), *Critical Media Literacy and Fake News in Post-Truth America* (BRILL 2018) 57
[33] Bernal n.1, 5. What is meant by the term social media and the emergence of social media is discussed in detail in later parts of this chapter.
[34] Digital, Culture, Media & Sport Committee n.30
[35] Anoosh Chakelian, 'Facebook releases Brexit campaign ads for the fake news inquiry – but what's wrong with them?' *NewStateman* (London, 27 July 2018) <https://www.newstatesman.com/politics/media/2018/07/facebook-releases-brexit-campaign-ads-fake-news-inquiry-what-s-wrong-them> accessed 14 November 2018
[36] Many of the fake news stories surrounding the Brexit campaign were also reported in tabloid newspapers.

Following the Brexit Referendum and the Presidential campaign in America, it publicly[37] emerged that Facebook had suffered a major data breach, resulting in 87 million Facebook profiles being harvested by Cambridge Analytica.[38] Aleksandr Kogan, a Psychology Professor at the University of Cambridge, created an app[39] on Facebook which allowed users to answer questions to determine their personality.[40] The terms of the app allowed for Kogan to harvest not only the profile information of those who chose to use the app, but also the personal information of all other online users who were friends with the original user of the app. The data collected was later sold to Cambridge Analytica, who were able to build political profiles of voters across the globe.[41] Cambridge Analytica were able to use these political profiles to build a further app which allowed them to target individuals with specific advertisements, suited to their political ideology. So, for instance during the Brexit campaign in the United Kingdom, a pro-Brexit organisation paid Cambridge Analytica to target voters with anti-European advertisements.[42] Many of these advertisements were linked to fake news.

---

[37] Facebook became aware of Cambridge Analytica in 2015 but it was only made public in 2018. See, Anthony Cuthbertson, 'Facebook knew about Cambridge Analytica data breach a year before Trump election' *The Independent* (London, 6 April 2018) <https://www.independent.co.uk/news/business/news/facebook-cambridge-analytica-trump-election-data-breach-mark-zuckerberg-a8292071.html> accessed 5 February 2019

[38] During the original investigation it was estimated 50 million profiles has been harvested. However, following an internal review by Facebook they have since confirmed that 87 million profiles were harvested by Cambridge Analytica. See, Guardian News, 'Mark Zuckerberg testifies before Congress' (*YouTube*, 10 April 2018) <https://www.youtube.com/watch?v=mZaec_mlq9M> accessed 14 January 2019

[39] App is short for an application. Apps are software programmes designed to perform specific functions.

[40] Carole Cadwalladr & Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' *The Guardian* (London, 17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 5 February 2019

[41] *Ibid.,*

[42] Patrick Greenfield, 'The Cambridge Analytica files: the story so far' *The Guardian* (London, 26 March 2018) <https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far> accessed 5 February 2019

The full extent of how fake news on social media sites influenced voters during these key political moments is unknown. In the United Kingdom a Parliamentary Committee was set up to investigate the effects of fake news during both the Brexit campaign and the General Election.[43] The committee highlighted the continuing threat of fake news on democracy, concluding that social media companies needed stronger regulation to ensure that they became legally liable for harmful content on their sites.[44] Yet fake news is not a new phenomenon unique to the digital age. Fake news has always been part of traditional forms of media. For instance, in 1993 a news story emerged stating that the European Union wanted to ban Prawn Cocktail crisps.[45] In fact, the European Commission had simply informed UK negotiators that they had missed out the 'production of specially flavoured crisps' when drafting a list of food products containing artificial sweeteners and flavours.[46]

Fake news has always been present within society, social media has just made it more prevalent than ever.[47] Indeed, social media content can reach millions in a short period of time:

> 'Kremlin-aligned media published significant numbers of unique articles about the EU referendum. 89 Up researchers analysed the most shared of the articles, and identified 261 with a clear anti-EU bias to the reporting. The two main outlets were RT and Sputnik, with

[43] Digital, Culture, Media & Sport Committee n.30, 363
[44] *Ibid.,* 89
[45] Commission, 'EC to ban prawn cocktail crisps' (*Euro Myths*, 16 January 1993) <https://blogs.ec.europa.eu/ECintheUK/ec-to-ban-prawn-cocktail-crips/> accessed 16 February 2019
[46] *Ibid*.,
[47] Tom Baldwin, *Ctrl Alt Delete: How Politics and the Media Crashed Our Democracy* (Oxford University Press 2018) 27

> video produced by Ruptly. The articles that went most viral had the heaviest antiEU bias. The social reach of these anti-EU articles published by the Kremlin-owned channels was 134 million potential impressions …'.[48]

The Internet as a Political Platform

Following the revolution of the Internet, there was a consensus that the online world should be beyond the control and interference of the state, as illustrated by John Perry Barlow:

> 'I declare the global social space we are building [the Internet] to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us, nor do you possess any methods of enforcement we have true reason to fear.'[49]

For Barlow, the Internet represented a space beyond the realms of government interference, free from political gain and outside the reach of the criminal law. His understanding of how the Internet should operate has been further supported by cyber-libertarians.[50] Those who endorse cyber-libertarianism suggest that the Internet is a separate entity from that of the physical world, and consequently, beyond interference from the state. Nevertheless, the expansion of changing technology and its dominance within society means that the Internet can no longer be considered as a separate entity from 'real-life'. Unlawful behaviour can be aided or solely conducted online. For example, as will be discussed in chapter four the

---

[48] Digital, Culture, Media & Sport Committee n.30, [243]
[49] John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (*Electronic Frontier Foundation*, 8 February 1996) <https://www.eff.org/cyberspace-independence> accessed 16 November 2018. Note this declaration was originally sent *via* email.
[50] For example, see the work of Esther Dyson, George Gilder, George Keyworth & Alvin Toffler, 'Cyberspace and the American Dream: A Magna Carta for the Knowledge Age' (1994) Future Insight <http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html> accessed 26 September 2018

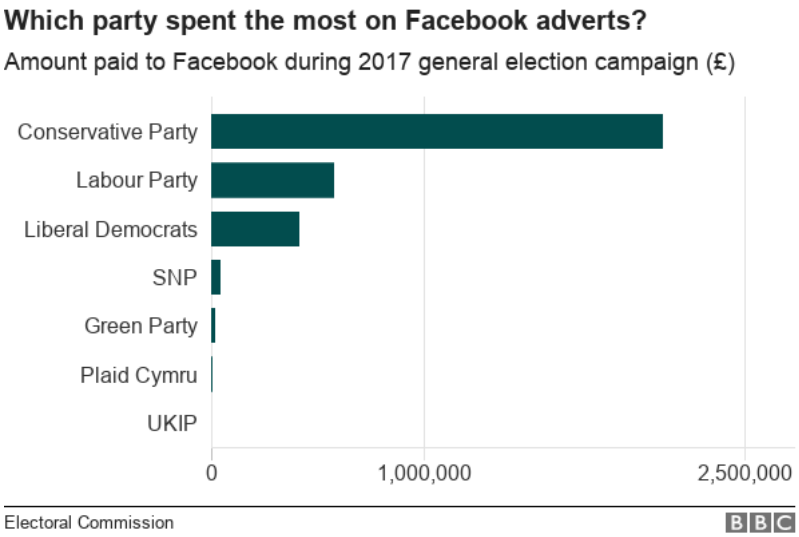
social media site Facebook was used as an external aid in the organisation of riots throughout the United Kingdom in 2011.

Since 1996, the separation of the Internet from that of 'real-life' has been eroded, to the point that it can no longer be fully considered as a space beyond the reach of government officials.[51] Recently, society has seen the use of the Internet and in particular social media, as a mechanism for political campaigning, as demonstrated in the 2017 General Election in the United Kingdom.[52]

Following an announcement by Theresa May, the then Prime Minister of the UK, calling for an early General Election, sites such as Twitter and Facebook quickly became utilised as a device for political campaigning.[53] In fact, the Conservative Party spent £2.1 million on advertising during the election campaign on Facebook, more than any other political party,[54] as demonstrated in figure two. For Margetts, '… social media platforms emerge[ed] as important players …'[55] in the 2017 General Election.

[51] Barry Wellman & Caroline Haythornthwaite, *The Internet in Everyday Life* (John Wiley & Sons 2008)
[52] Helen Margetts, 'Why Social Media May Have Won the 2017 General Election' (2017) 88(3) The Political Quarterly 386
[53] Mike Wendling, 'Election 2017: Was it Facebook wot swung it?' *The BBC* (London, 10 June 2017) <https://www.bbc.co.uk/news/blogs-trending-40209711> accessed 16 November 2018
[54] Peter Walker, 'Tories spent £18.5m on election that cost them majority' *The Guardian* (London, 19 March 2018) <https://www.theguardian.com/politics/2018/mar/19/electoral-commission-conservatives-spent-lost-majority-2017-election> accessed 16 November 2018
[55] Margetts n.52, 389

Figure 2: *Expenditure by political group on Facebook advertisements during the 2017 General Election.* [56]



The use of social media during the 2017 General Election also exposed a darker side to the net, online abuse. Throughout the election campaign period, MPs in particular female politicians were subjected to highly abusive commentary online. Diane Abbot the Labour Shadow Home Secretary, was the most abused MP on Twitter[57] during the campaign period, receiving more than 50% of all abusive tweets sent throughout the campaign:[58]

> 'I have had death threats, and people tweeting that I should be hanged "if they could find a tree big enough to take the fat bitch's weight". There was an English Defence League-affiliated Twitter account- #burnDianeAbbot. I have had rape threats, and been described as a "pathetic useless fat black piece of shit", an "ugly, fat black bitch", and a "nigger"- over and over again.'[59]

[56] Joey D'Urso, 'Who spent what on Facebook during 2017 election campaign?' *The BBC* (London, 31 March 2018) <https://www.bbc.co.uk/news/uk-politics-43487301> accessed 16 November 2018

[57] Twitter is discussed in detail in later parts of this chapter.

[58] Jessica Elgot, 'Diane Abbott more abused than any other MPs during election' *The Guardian* (London, 5 September 2017) <https://www.theguardian.com/politics/2017/sep/05/diane-abbott-more-abused-than-any-other-mps-during-election> accessed 16 November 2018

[59] Rowena Mason, 'Diane Abbott on abuse of MPs: "My staff try not to let me go out alone"' *The Guardian* (London, 19 February 2017)

Despite the abuse experienced by MPs during the 2017 UK General Election, commentators such as Myers argued that online abuse aimed at MPs is part of a healthy democracy, where citizens should be able to criticise politicians online.[60] For Myers what MPs define as abuse is simply '… criticism, ridicule and insult'.[61] Despite this, as will be exposed in later parts of this thesis, online abuse is a threat to democracy. It can have a direct impact on a person choosing to enter the world of politics, whilst silencing political campaigning. The effects of online abuse are discussed in detail in later sections of this chapter.

The Internet as a Public Space

The Internet was, and still is widely considered, a public space whereby freedom of speech will prevail:

> 'Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.'[62]

Free speech has become somewhat the trump card to abusive commentary online.[63] As detailed in chapter seven free speech is considered the right to hold an opinion which can be expressed in any medium required by the speaker. For libertarians there should be no limit on a person's expression.[64] Whereas pro-regulators suggest that while the user is present in the physical

---

<https://www.theguardian.com/politics/2017/feb/19/diane-abbott-on-abuse-of-mps-staff-try-not-to-let-me-walk-around-alone> accessed 6 March 2017

[60] Fraser Myers, 'We must have the right to insult politicians' (*Spiked*, 25 September 2018) <https://www.spiked-online.com/2018/09/25/we-must-have-the-right-to-insult-politicians/> accessed 16 February 2019

[61] *Ibid.,*

[62] Baldwin n.47, 44

[63] Zia Akhar, 'Malicious communications, media platforms and legal sanctions' (2014) 20(6) Computer and Telecommunications Law Review 179, 181

[64] See for example Barlow n.49

world, the Internet cannot be beyond the realms of government interference.[65]

For free speech libertarians the Internet should be beyond the reach of the law to protect freedom of expression. The World Wide Web has become integral to freedom of expression, it allows users to challenge the State, create change within society, and brings individuals with similar ideas together. The use of the World Wide Web has now become paramount to social change. Nevertheless, as mentioned above since the creation of the Internet and the World Wide Web, it has been used as a weapon to target other users.

In recent years MPs,[66] celebrities,[67] campaigners,[68] academics,[69] and other general Internet users,[70] have become targets for Internet trolls.[71] Free speech is often quoted at those who are subjected to this form of abuse

[65] Bernal n.1, 19
[66] Elgot n.58
[67] Caroline Davies, 'Katie Price urges MPs to act after "horrific" online abuse of son' *The Guardian* (London, 6 February 2018) <https://www.theguardian.com/media/2018/feb/06/katie-price-urges-mps-to-make-online-abuse-a-criminal-offence> accessed 1 May 2018
[68] Alexandra Topping, 'Jane Austen Twitter row: two plead guilty to abusive tweets' *The Guardian* (London, 7 January 2014) <https://www.theguardian.com/society/2014/jan/07/jane-austen-banknoteabusive-tweets-criado-perez> accessed 10 October 2016
[69] Ben Dowell, 'Mary Beard suffers "truly vile" online abuse after Question Time' *The Guardian* (London, 21 January 2013) <https://www.theguardian.com/media/2013/jan/21/mary-beard-suffers-twitter-abuse> accessed 26 November 2018
[70] Nadia Khomami, 'NSPCC records 88% rise in children seeking help for online abuse' *The Guardian* (London, 14 November 2016) <https://www.theguardian.com/society/2016/nov/14/nspcc-records-88-rise-in-children-seeking-help-for-online-abuse> accessed 26 November 2018
[71] Trolls can be defined as, '[a] person who creates controversy in an online setting (typically on a social networking website, forum, comment section, or chatroom), disrupting conversation as to a piece of content by providing commentary that aims to provoke an adverse reaction.' See, Law Commission n.15, 10

online, with arguments being put forward that the Internet should be beyond the realms of the criminal law.[72] However, free speech in the form of abuse can be stifling on freedom of expression. By abusing others online sectors of society are having their opinions and voices silenced. This directly affects those who are subjected to online abuse as their own right to free speech is reduced. Online abuse affects other rights such as privacy. Whereas some commentators[73] maintain that privacy does not exist online, this is disputed by Bernal: '[P]eople do have an expectation to privacy even in what might be generally be called "public" space on the Internet.'[74] The issue of privacy in the digital world is discussed further in chapter seven.

The Internet as a Communications Device

The expansion of changing technology has not only changed how we obtain information, adapted political campaigns or indeed altered how we shop, it has also transformed how society communicates.[75] In 1971 the first email between two computers was transmitted.[76] Since then, technological advances have revolutionised speech, in the form of social media, online

[72] Barlow n.49
[73] *Ibid.,*
[74] Bernal n.1, 16
[75] Law Commission n.15, [1.34]
[76] Centre for Computing History, '1971: First Network Email sent by Ray Tomlinson' (*Centre for Computing History*, 2016) <http://www.computinghistory.org.uk/det/6116/First-e-mail-sent-by-Ray-Tomlinson/> accessed 27 November 2018

blogging,[77] vlogging[78] and live video broadcasts.[79]

The use of the Internet as a communications medium has been on the increase since the early 1990s:

> 'Technological advancement in the 19th century sparked a revolution in the speed of communication. The invention of the telegraph was the first form of electrical telecommunication that had this effect. Subsequent innovations such as the telephone, radio, television, the Internet, and most recently, the emergence of social media, have radically transformed the way we communicate.'[80]

By 2015 it was estimated that there were over 200 websites whereby users could create online profiles and communicate instantly with others, commonly referred to as social media.[81] Social media as discussed below, allows users to instantly communicate not only with their friends, but in some cases with the general public.[82] Throwaway comments which in the past would have gone undocumented can now be actively shared across the globe in a matter of minutes.[83]

Summary

[77] 'An online journal, or "web log", usually maintained by an individual or business and with regular entries of content on a specific topic, descriptions of events, or other resources such as graphics or videos.' See, Law Commission n.23, 5
[78] 'Utilising video recordings to tell a story or to report on information, common on video sharing networks such as YouTube (a shortening of "video web log").' See, Law Commission n.15, 10
[79] Note, this is not a definitive list.
[80] Law Commission n.15, [2.29]
[81] Laura Scaife, *Handbook of Social Media and the Law* (Routledge 2015) 4
[82] For instance, Twitter allows comments to be made which are publicly viewable to those without a Twitter account.
[83] For example, in 2015 an individual tweeted the following: 'Going to Africa. Hope I don't get AIDS [*sic*]. Just kidding. I'm white!' Following the tweet being actively shared across Twitter, the individual was arrested and subsequently lost her job. See, Jon Ronson, 'How One Stupid Tweet Blew Up Justine Sacco's Life' *The New York Times Magazine* (New York, 12 February 2015) <https://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html> accessed 5 February 2019

As Bernal argues the modern Internet has become integral to society.[84] It has impacted on all areas of social life. For instance, we have seen the use of websites to promote change within society, such as the recent '#MeToo' campaign, which highlighted the ongoing issues of sexual violence and assault across the world.[85] Many of these campaigns have been aided by social media. Yet social media has a darker side whereby users can be actively abused and targeted by others online.

Social Media: An Explanation

The term social media covers a range of online conducts for instance, blogging, video sharing sites and virtual world reality games can all fall within the definition of social media.[86] For the purpose of this thesis the term social media is used to refer to websites/devices which allow users to create their own profiles and commentary, whilst also allowing individuals to communicate instantly with others.

Though there is no one true definition of social media, it has come to be accepted that social media is:

> 'the ability to share, to co-operate, with one another, and to take collective actions, all outside the framework of traditional institutions and organisations.'[87]

[84] Bernal n.1, 19
[85] Bri Lee, 'Sharing our stories is the strength at the heart of #MeToo. We must repeal gag laws' *The Guardian* (London, 19 November 2018) <https://www.theguardian.com/commentisfree/2018/nov/19/sharing-our-stories-is-the-strength-at-the-heart-of-metoo-we-must-repeal-gag-laws> accessed 27 November 2018
[86] Scaife n.81, 8-9
[87] Clay Shirky, *Here comes everyone* (Penguin 2008) 20. For a discussion on different definitions of social media see, Christian Fuchs, *Social Media a Critical Introduction* (Sage Publications 2014) 35-37

As outlined by the Law Commission there are several fundamental characteristics associated with social media, including the ability to generate a profile and actively share information.[88] The first generation of social media was created in the early 1990s, through websites which allowed users to post comments on bulletin-boards.[89] Following a demand for online services in which individuals could connect with others, new social media sites were created aimed at connecting online users.

The first form of social media as society knows it today, emerged in 1997, 'SixDegrees.com', in which users of the site could connect with friends and family.[90] Following the initial success of SixDegrees other websites started to emerge based on a similar format, such as that of 'Hub Culture' and 'MySpace'.[91] Since the creation of SixDegrees, social media usage has been on the increase. In 2017, 66% of over 16s in the UK had access to at least one social media site, this increased to 96% for those aged between 16 and 24.[92] Two of the biggest forms of social media today, are Facebook and Twitter.

On 4 February 2004 Mark Zuckerberg, a college student at Harvard University, alongside several other students, launched 'TheFacebook', later to be renamed 'Facebook'. The initial purpose of Facebook was to create a

[88] Law Commission n.15, [2.32]
[89] Scaife n.81, 4
[90] *Ibid.,*
[91] *Ibid.,*
[92] Office of National Statistics, 'Internet access – households and individuals, Great Britain: 2017' (*Office of National Statistics*, 3 August 2017) <https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2017> accessed 26 November 2018

social media site as a communications mechanism for students at Harvard University, with the site later being made available to all higher education students in the Boston area.[93] In 2006 Facebook was released to the world, with anyone who claimed[94] to be over 13 years of age being able to create a Facebook page.

Facebook, since its original launch in 2004, has become the biggest social media company today.[95] The website '… operates as a social networking site based on interconnection with other users to generate content.'[96] Here users must register with the site and build personal profiles of themselves, which can include, likes and dislikes, a picture of themselves, their date of birth, and other unique information such as where they were educated. In fact, Facebook is built on the premise of getting its users to reveal private information about themselves.

By 2016 Facebook had expanded to become the sixth-most valuable public company in the world. [97] In June 2017 Mark Zuckerberg announced *via* Facebook, that the social media company now had 2 billion users, averaging

[93] Sarah Phillips, 'A brief history of Facebook' *The Guardian* (London, 25 July 2007) <https://www.theguardian.com/technology/2007/jul/25/media.newmedia> accessed 26 November 2018
[94] Very little is done to verify the age of users on Facebook. Recently, Facebook has announced that it will do more to reduce underage usage. See, Josh Constine, 'Facebook and Instagram change to crack down on underage children' (*Tech Crunch*, 2018) <https://techcrunch.com/2018/07/19/facebok-under-13/> accessed 29 November 2018
[95] Josh Constine, 'Facebook now has 2 billion monthly users … and responsibility' (*Tech Crunch*, 2017) <https://techcrunch.com/2017/06/27/facebook-2-billion-users/> accessed 29 November 2018
[96] Scaife n.81, 9
[97] Smartt n.2, 79

around 580,000 new users each day.[98] In the United Kingdom alone 32.6 million citizens are active Facebook users.[99]

Similar trends have also been mirrored with other social media companies such as Twitter. Twitter emerged in 2006 as an alternative form of social media. Like that of Facebook, Twitter users can create online profiles though their comments, or tweets as they have become known, were originally limited to 140 characters.[100] In 2015, 500 million tweets were sent every day on Twitter, averaging around 6000 tweets per second.[101]

The creation of social media has had a direct effect on how individuals communicate. In turn, traditional forms of reducing speech, such as that of bullying, are now present in the online world.[102] In recent years, the issue of online abuse has dominated much of society, resulting in research being undertaken to expose the extent of this phenomenon, both here in the United Kingdom and elsewhere. The following discussion will highlight recent research exposing the growing trend in online abuse. This will allow for the foundations of this thesis to be set by examining whether the current criminal law framework in England and Wales,[103] adequately protects individuals from

---

[98] James Titcomb, 'Facebook now has 2 billion users, Mark Zuckerberg announces' *The Telegraph* (London, 27 June 2017) <https://www.telegraph.co.uk/technology/2017/06/27/facebook-now-has-2-billion-users-mark-zuckerberg-announces/> accessed 29 November 2018

[99] Mark Sweney, 'Is Facebook for old people? Over-55s flock in as the young leave' *The Guardian* (London, 12 February 2018) <https://www.theguardian.com/technology/2018/feb/12/is-facebook-for-old-people-over-55s-flock-in-as-the-young-leave> accessed 29 November 2018

[100] This has since expanded to 280 characters.

[101] Smartt n.2, 79

[102] See, Law Commission n.15, [1.33]

[103] As noted in the Introduction, the foundation of this thesis will examine the criminal law in England and Wales, as opposed to the whole of the United Kingdom. This is simply because

online abuse.

Online Abuse

To examine if the current criminal law framework is adequate in protecting those who are subjected to abusive commentary online, first the meaning of online abuse must be examined. Like that of social media, there is no one true definition of online abuse. Studies which have examined the extent of abusive behaviour online all use different definitions of the term. The following discussion will outline some of the meanings given to this type of behaviour, before turning to look at the extent of online abuse today.

There is no clear consensus as to the meaning of online abuse. In fact, the term 'abuse' is ambiguous with no agreement in law as to the meaning of abusing another. In 1995 the Law Commission during their report into Adult Social Care attempted to crystallise the meaning of abuse:

> '… ill-treatment (including sexual abuse and forms of ill-treatment that are not physical); the impairment of, or an avoidable deterioration in, physical or mental health; and the impairment of physical, emotional, social or behavioural development.'[104]

Similarly, the Oxford Dictionary gives two definitions of abuse:

> '"Abusive" is defined variously in the Oxford English Dictionary as first, treating someone with cruelty or violence, especially regularly or repeatedly, or secondly, speaking to someone in an insulting or offensive way.'[105]

Despite a lack of a consistent definition, it is clear that there are key characteristics associated with what can be considered as abuse. For

Scotland and Northern Ireland have their own private laws governing certain criminal behaviours.

[104] Law Commission, *Adult Social Care* (Law Com No 326, 1995) [9.51]

[105] Law Commission n.15, [1.11]

instance, physical, sexual or mental ill-treatment fall within the definition of abuse.[106]

Though the definitions above can be used to describe abuse online, their application to online abuse may be considered as too wide. The Oxford English Dictionary considers abuse to include offensive behaviour. However, to criminalise offensive behaviour online could be considered as limiting free speech. As affirmed in *Handyside v United Kingdom*[107] citizens have the right to be offensive.[108] Therefore, a narrower definition of online abuse is needed.

For the National Society for the Prevention of Cruelty to Children (NSPCC), online abuse, in its simplest form refers to the ill-treatment of another which takes place online.[109] Like that of the Oxford English Dictionary, the definition given by the NSPCC can be considered as too wide. For Lewis, Rowe and Wiper, online abuse refers to 'hostile communications', which are characterised by certain online conduct.[110] Like that of traditional forms of abuse, certain online behaviours can fall within the definition of online abuse. Some of these behaviours stem from traditional forms of mistreatment, which have now been mirrored in an online context. For example, bullying which

---

[106] See also, Europe Institute for Gender Equality, 'Cyber violence against women and girls' (*Europe Institute for Gender Equality*, 2017) <eige.europa.eu/sites/default/files/.../cyber_violence_against_women_and_girls.pd> accessed 15 February 2017

[107] *Handyside v United Kingdom* (1976)1 EHRR 737

[108] *Ibid.,* [49]

[109] NSPCC, 'Online abuse: What is online abuse?' (*NSPCC*, 2018) <https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/> accessed 6 December 2018

[110] Ruth Lewis, Michael Rowe & Clare Wiper, 'Online Abuse of Feminists as An Emerging form of Violence Against Women and Girls' (2017) 57(6) The British Journal of Criminology 1462

would once take place only in the physical world, can now be conducted wholly online and has been coined cyberbullying. In addition, new ways to taunt and abuse another have emerged online.

In 2018 the Law Commission examined abusive and offensive commentary online. Here, like other studies which will be discussed in detail in later chapters, the committee did not give an overall definition of online abuse. Instead, they defined certain conduct which can be associated with abusing another online. For example:

- Cyberbullying- The use of the Internet to continually taunt another. This form of behaviour is commonly associated with the younger generation. It is very similar to traditional forms of bullying, but it can take place solely online or it can be aided by digital technology;
- Cyberstalking- Stalking is defined as '… repeated incidents, which may or may not individually be innocuous acts, but combined undermine the victim's sense of safety and cause distress, fear or alarm.'[111] Cyberstalking refers to the situation whereby the behaviour takes place in an online context;
- Revenge pornography- The distribution of explicit images or videos of another to cause the person in the images or video distress. Though this behaviour can occur offline, it has evolved since the creation of the World Wide Web;
- Doxing- Publishing private information about another online such as home addresses, with the intention to cause the victim distress; and

[111] Europe Institute for Gender Equality n.106

- Dogpiling- Encouraging other Internet users to target a specific individual. This type of behaviour has commonly been used against individuals based in the public domain.

The above behaviours are not definitive but are conducts which are discussed in more detail throughout this thesis. Upon review of the literature, for the purpose of this thesis, online abuse is considered:

> Insulting and hostile behaviour aimed at another online which causes the deterioration of another's physical and mental wellbeing; threats of physical and/or sexual violence; insulting and hostile behaviour aimed at another because of their (if real or presumed) gender, race, ethnicity, religion, national origin, gender identity, sex, disability or sexual orientation.

Though there are other definitions available, this definition has been generated as it covers threats of physical or sexual violence, hate speech and reflects the mental anguish associated with online abuse.

The Extent of Online Abuse

Research has started to emerge in recent years exposing the extent of abusive conduct online, though its true scale is unknown. For Essex Police Chief Constable Stephen Kavanagh, the current research on online abuse is only 'the tip of the iceberg', with police forces unable to cope with the scale of abuse that is currently taking place online.[112]

In October 2017 the BBC released a Freedom of Information request exposing the number of police reports made between 2015 and 2016, where malicious communications were the main element of the crime being

[112] The BBC, 'Teenager's life "ruined" by Live.me and Twitter "trolls"' *The BBC* (London, 24 October 2017) <http://www.bbc.co.uk/news/uk-england-41693437> accessed 30 January 2018

complained about.[113] Thirty-eight out of forty-two police forces responded to the request. The BBC uncovered that between 2015 and 2016, there had been an increase of 36,462 police reports involving malicious communications. Yet the findings of the BBC are only a glimpse of the true extent of online abuse taking place across the globe.

Facebook, the biggest social media company today has been under increasing pressure to actively deal with unlawful behaviour which takes place on its platform:

> 'You [Mark Zuckerberg, Facebook CEO] have to ask yourself how you will be remembered - as one of the three big Internet giants together with Steve Jobs and Bill Gates who have enriched our worlds and our societies. Or on the other, in fact, a genius who created a digital monster that is destroying our democracies and our societies.'[114]

Consequently, the company has since released a report exposing the scale of online abuse on its site. Facebook, over two three month periods, recorded comments and images which breached their community guidelines.[115] These comments and images were then categorised into groups. For instance, graphic violence, spam, hate speech, adult nudity and sexual conduct.[116]

---

[113] *Ibid*., Here, the term 'malicious communication' was used as a generic term for abusive commentary sent online.

[114] Alexis C Madrigal, 'A Belgian Legislator Berates and Scoffs at Mark Zuckerberg' *The Atlantic* (Boston, 22 May 2018) <https://www.theatlantic.com/technology/archive/2018/05/a-belgian-legislator-berates-and-scoffs-at-mark-zuckerberg/560960/> accessed 16 August 2018

[115] Facebook's community guidelines outline the terms of service for its site. In essence, it illustrates what conduct is and is not permitted by its users. For an in-depth discussion of Facebook's community guidelines, see chapter three.

[116] Guy Rosen, 'Facebook Publishes Enforcement Numbers for the First Time' (*Facebook*, 15 May 2018) <https://newsroom.fb.com/news/2018/05/enforcement-numbers/> accessed 9 December 2018. See also, Dave Lee, 'Facebook details scale of abuse on its site' *The BBC* (London, 15 May 2018) <https://www.bbc.co.uk/news/technology-44122967> accessed 9 December 2018

In the first three month period, October 2017 to December 2017, the company removed 1.2 million 'pieces' of content from its platform which were considered to be graphically violent.[117] In the following three month period, January 2018 to March 2018, this increased by 183% to 3.4 million 'pieces'.[118] In spite of this, and warnings given by Essex Police Chief Constable Stephen Kavanagh, the content removed by Facebook was only the 'tip of the iceberg'. Later research undertaken by Facebook found that for every 10,000 posts placed during the same full six-month period, 27 abusive posts had been overlooked by the company.[119]

Facebook also uncovered a growing trend of hate-related speech on its site during the same research period. For Facebook hate speech is:

> '… a direct attack on people based on what we [Facebook] call protected characteristics - race, ethnicity, national origin, religious affiliation, sexual orientation, caste, sex, gender, gender identity and serious disease or disability.'[120]

During the first data collection period, Facebook removed 1.6 million 'pieces' of content which were considered to breach the company's guidelines in relation to hate speech.[121] In the second three month period this increased to 2.5 million.[122] Facebook's definition of hate speech is significantly broader than the definition located in the legal system of England and Wales, where

---

[117] *Ibid.,*
[118] *Ibid.,*
[119] *Ibid.,*
[120] Facebook, 'Community Standards: Hate Speech' (*Facebook*, 2018) <https://www.facebook.com/communitystandards/hate_speech> accessed 9 December 2018
[121] Rosen n.116
[122] *Ibid.,*

hate speech is considered commentary that is '… motivated by hostility or demonstrates hostility towards the victim's disability, race, religion, sexual orientation or transgender identity.'[123]

Recently in the United Kingdom, there has been a drive to change the definition of protected characteristics to include a person's gender or sex. Currently, a person who targets another because of their sex is not recognised as committing a hate crime. Nevertheless, Nottinghamshire Police Force since 2016 has started recording crime in which gender is a motivating factor.[124] Since then, arguments have been put forward that this approach should be implemented across police forces in England and Wales.[125]

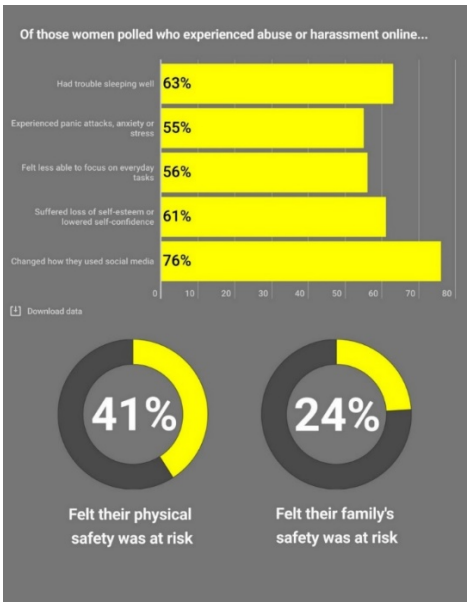
In 2017 Amnesty International, a human rights organisation, conducted an IPSOS[126] poll examining the extent to which women are abused *via* social media.[127] The poll was conducted across eight states, including Denmark, Italy, New Zealand, Poland, Spain, Sweden, the UK and the USA, looking at the online experiences of women aged between 18 and 55. 23% of those surveyed stated that they had, on at least one occasion, experienced online

[123] The Crown Prosecution Service, 'Hate Crime' (*CPS.gov*, 2018) <https://www.cps.gov.uk/hate-crime> accessed 9 December 2018
[124] The BBC, 'Nottinghamshire Police records misogyny as a hate crime' *The BBC* (London, 13 July 2016) <https://www.bbc.co.uk/news/uk-england-nottinghamshire-36775398> accessed 16 February 2019
[125] Libby Brooks, 'Review brings misogyny as a hate crime a step closer' *The Guardian* (London, 6 September 2018) <https://www.theguardian.com/society/2018/sep/05/first-step-to-misogyny-becoming-a-hate-called-amazing-victory> accessed 16 February 2019
[126] IPSOS is a global market research firm.
[127] Amnesty International, 'Amnesty reveals alarming impact of online abuse against women' (*Amnesty International*, 20 November 2017) <https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/> accessed 9 December 2018

abuse or harassment.[128] This had significant effects on those who had been subjected to online abuse as shown further in figure three. For instance, 55% of participants experienced stress, anxiety or panic attacks directly linked to the abusive behaviour they were subjected to online.[129]

One of the most significant findings of the study uncovered that of those women who had been subjected to online abuse, 76% had changed the way in which they utilised social media.[130] Online abuse which results in the user changing their online habits can have a direct effect on a person's right to freedom of expression, as outlined in chapter seven. Freedom of expression in the form of abusive online commentary can, in fact, reduce another's right to free speech.

Figure 3: The effects on women who were subjected to online abuse. [131]



[128] *Ibid.,*
[129] *Ibid.,*
[130] *Ibid.,*
[131] *Ibid.,*

During the 2017 General Election in the UK as outlined in previous sections of this chapter, social media was at the forefront of many MPs campaign strategies. However, social media was also used to target MPs during the campaign period. Following the 2017 General Election, Amnesty International conducted research directly examining the scale of abuse during the election campaign.[132] They found that between 1 January 2017 and 8 June 2017, 900,223 tweets were sent to 177 female MPs, of this 25,688 were deemed abusive.[133]

Research studies such as those above, illustrate the growing issue of online abuse within society. These studies however do not clearly define what they consider to be abusive conduct, leaving flaws within their findings. Despite this, it is clear more needs to be done to tackle online abuse. The following sections will expose the extent of specific behaviours associated with online abuse which have been aided by social media.

Cyberbullying

Not only has the Internet created new and unique ways to taunt another, behaviour which was once confined to the physical world has now emerged

[132] Amnesty International UK, 'Black and Asian women MPs abused more online' (*Amnesty International*, 2017) <https://www.amnesty.org.uk/online-violence-women-mps> accessed 9 December 2018. See also, Laura Bliss, 'Abuse of women MPs is not just a scandal – it's a threat to democracy' *The Conversation* (London, 17 July 2017) <https://theconversation.com/abuse-of-women-mps-is-not-just-a-scandal-its-a-threat-to-democracy-80781> accessed 9 December 2018

[133] *Ibid.,*

online.[134] This is true with cyberbullying.[135] Cyberbullying takes the form of traditional bullying behaviour but is conducted online.

Each year Ditch the Label with the help of educational institutions conducts a survey exposing the extent of bullying in the United Kingdom. In recent years they have included the concept of cyberbullying. In 2016 they found that 65% of participants had experienced some form of cyberbullying, an increase of 3% on the previous year.[136] By 2018 66% of participants had been subjected to cyberbullying, an increase of 1% since 2016.[137] Cyberbullying has continued to be a problem within the educational sector, calling for the Government to announce compulsory lessons in schools teaching young people about social media and bullying online.[138]

As will be discussed in later chapters, educational institutions have been slow in creating effective and knowledgeable digital literacy workshops, meaning in many cases young people do not fully comprehend the legal

---

[134] Press Association, 'Social media-related crime reports up 780% in four years' *The Guardian* (London, 27 December 2012) <https://www.theguardian.com/media/2012/dec/27/social-media-crime-facebook-twitter> accessed 18 October 2016. The types of conduct reported to the police varied, but it included reports of credible threats of violence, menacing messages and sexual offences.
[135] Law Commission n.15, [1.33]
[136] Ditch the Label, 'The Annual Bullying Survey 2016' (*Ditch the Label*, 2016) 14 <http://www.ditchthelabel.org/wp-content/uploads/2016/04/Annual-Bullying-Survey-2016-Digital.pdf > accessed 18 October 2016. See also, Ditch the Label, 'The Annual Bullying Survey 2015' (*Ditch the Label*, 2015) 18 <http://ditchthelabel.org/downloads/abs2015.pdf> accessed 26 February 2016
[137] Ditch the Label, 'The Annual Bullying Survey 2018' (*Ditch the Label*, 2018) 13 <https://www.ditchthelabel.org/wp-content/uploads/2018/06/The-Annual-Bullying-Survey-2018-2.pdf> accessed 12 December 2018
[138] HM Government, 'Government response to the Internet Safety Strategy Green Paper' (*Gov.uk*, May 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf > accessed 27 July 2018

ramifications of their online behaviour.[139] For instance a study conducted by Powell-Jones of 184 young people, revealed a lack of understanding in participants concerning the law surrounding indecent images, hate speech and online abuse.[140]

Yet cyberbullying can have detrimental effects on those who are subjected to it:

> 'The psychological harm inflicted by cyberbullying, just like bullying, is reflected in low self-esteem, school failure, anger, anxiety, depression, school avoidance, school violence, and suicide.'[141]

Whereas traditional forms of bullying in young people are associated with the 'playground', cyberbullying can be relentless and can occur around the clock. In 2012 Erin Gallagher (13) took her own life after being continually subjected to anonymous abusive comments on the social media site, ASK.FM.[142] Similarly, research conducted by John *et al* found that individuals who were bullied online were twice as likely to self-harm or attempt suicide.[143]

---

[139] Holly Powell-Jones, 'Online abuse: teenagers might not report it because they often don't see it as a problem' *The Conversation* (London, 7 May 2019) <https://theconversation.com/online-abuse-teenagers-might-not-report-it-because-they-often-dont-see-it-as-a-problem-116479> accessed 26 June 2019

[140] Holly Powell-Jones, 'Research Findings' (*Online Media Law UK*, 2019) <https://www.onlinemedialawuk.com/phd-research> accessed 26 June 2019. See also, Holly Powell-Jones, 'How do young people interpret and construct risk in an online context?' (PhD Thesis, City London University 2018)

[141] Qing Li, 'Cyberbullying in High Schools: A Study of Students' Behaviors and Beliefs about This New Phenomenon' (2010) 19(4) Journal of Aggression, Maltreatment & Trauma 372, 374

[142] Greg Harkin, 'Family devastated after tragic Erin (13) takes own life after vicious online bullying' *Irish Independent* (Dublin, 29 October 2012) <https://www.independent.ie/irish-news/family-devastated-after-tragic-erin-13-takes-own-life-after-vicious-online-bullying-28824852.html> accessed 12 December 2018

[143] Ann John *et al*, Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review (2018) 20(4) J Med Internet Res <https://www.jmir.org/2018/4/e129/> accessed 12 December 2018. See also, Sarah Knapton n.85

Online harassment and stalking

In recent years social media has been used to harass and stalk others online. Harassment as discussed further in chapter four refers to the continued unwanted contact between an individual and another to cause alarm or distress.[144] Whereas stalking has no specific definition, and instead a list of behaviours has been produced which can amount to stalking:

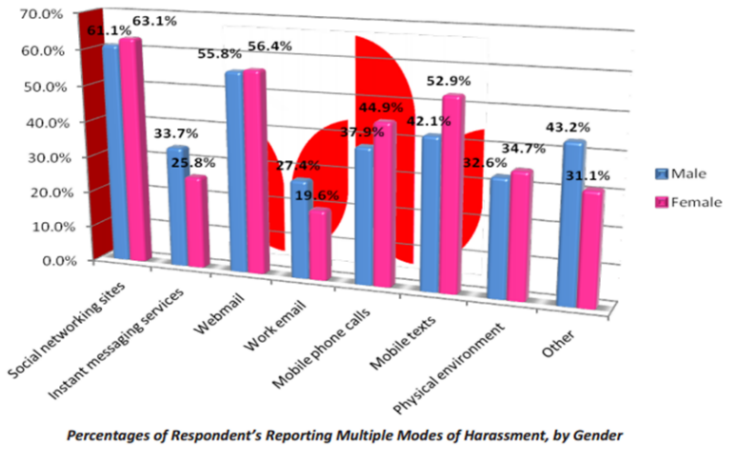
> 'The following are examples of acts or omissions which, in particular circumstances, are ones associated with stalking- (a) following a person; (b) contacting, or attempting to contact, a person by any means; (c) publishing any statement or other material - (i) relating or purporting to relate to a person, or (ii) purporting to originate from a person; (d) monitoring the use by a person of the Internet, email or any other form of electronic communication; (e) loitering in any place (whether public or private); (f) interfering with any property in the possession of a person; [and] (g) watching or spying on a person.'[145]

Like that of cyberbullying, stalking and harassment can now be aided or solely conducted online. The conduct of stalking and harassing another *via* the Internet is now commonly referred to as cyberstalking or cyber harassment. As cyber harassment and cyberstalking are inherently interlinked, as legally in England and Wales a person cannot be stalked if harassment is not present, there continues to be difficulties in establishing the boundary between these two behaviours. The distinction between cyber harassment and cyberstalking will be further discussed in chapter four.

[144] Protection from Harassment Act 1997 section 1
[145] Protection from Harassment Act 1997 section 2A(3)

In 2003 Bocij conducted a survey examining the extent of cyberstalking online.[146] Bocij, using an email snowballing sample,[147] surveyed 169 participants aged 16 to 84 years old.[148] To conclude if participants had been subjected to cyberstalking, Bocji asked a number of questions related to certain types of online conduct associated with stalking online. For example, the receiving of threatening or abusive emails and the spread of false information online. Using this approach Bocji was able to conclude that 21.9% of his participants had been subjected to what he deemed as cyberstalking.[149] The research undertaken by Bocji indicates that even before the creation of Facebook and Twitter, cyberstalking behaviour was an issue within society.

Figure 4: *Communication devices used to abuse others online as found by Brown, Maple and Short.* [150]



[146] Paul Bocij, 'Victims of Cyberstalking: An Exploratory Study of Harassment Perpetrated via the Internet' (2003) 8(10) First Monday <http://firstmonday.org/ojs/index.php/fm/article/view/1086> accessed 30 October 2016. This statistic was generated using a rigid definition of cyberstalking.
[147] In a snowballing sample the researcher recruits a few participants, who in turn recommend others to take part in the study. See, Earl Babbie, *The Basics of Social Research* (Cengage Learning 2007) 205
[148] Bocij n.146
[149] *Ibid.,*
[150] Brown, Maple & Short n.152

Social media has revolutionised how cyberstalking and cyber harassment can be conducted. Research undertaken on behalf of Bedfordshire University by Brown, Maple and Short, found that of the 353 participants who took part in their survey 92% had been subjected to some form of cyberstalking or cyber harassment, of this, 94.1% of participants had been left in some form of distress.[151] In addition, the work of Brown, Maple and Short exposed just some of the ways in which a person can harass or stalk another online, illustrated in figure four. Yet it was not until 2012 that stalking, and harassment became separate criminal offences.[152]

Despite a consensus that online harassment and stalking are on the increase, prosecutions under the Protection from Harassment Act 1997, which criminalises these types of behaviours in England and Wales, has decreased.[153] Each year the CPS conducts a report examining violence against women and girls in England and Wales. The 2017 report exposed that the number of prosecutions brought under the Protection from Harassment Act relating to stalking and harassment had decreased by 8.4% compared to the previous year.[154] Yet a BBC Freedom of Information request

[151] Antony Brown, Carsten Maple & Emma Short, 'Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey' (*University of Bedfordshire National Centre for Cyberstalking Research*, 2011) 9 <https://www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf> accessed 25 October 2016

[152] Before 2012 stalking and harassment were considered similar offences and criminalised under section 2 of the Protection from Harassment Act.

[153] The BBC, 'Cyberbullying and trolling reports to Welsh police double' *The BBC* (London, 24 October 2017) <https://www.bbc.co.uk/news/uk-wales-41729206> accessed 10 December 2018

[154] The Crown Prosecution Service, 'Violence against women and girls report: tenth edition' (*CPS.gov*, 2017) 7 <https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2017.pdf> accessed 19 February 2017. Please note, there is an issue with these statistics. As uncovered by the Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate, police forces and the CPS have confused the definitions

found an 85% rise in reports made to the police concerning online harassment and trolling.[155] It can be suggested that despite the increase in reports made to the police relating to cyberstalking and cyber harassment, fewer prosecutions are being pursued in the criminal justice system.

As in the case with cyberbullying, it is clear that cyberstalking and cyber harassment are becoming increasingly problematic for society, with these behaviours having significant effects on a person's mental wellbeing. The problematic nature of cyberbullying, cyber harassment and cyberstalking is further reflected when examining revenge pornography.

Revenge pornography

Revenge pornography is the distribution of sexualised images to cause distress upon another. Though anyone can become a victim of revenge pornography it disproportionally affects women more than men, and is considered the ultimate humiliation that can be placed upon a person.[156] Though revenge pornography is not necessarily a new behaviour associated with the digital age, revenge porn has been made easier with the aid of new technology. For example, in 2010 the first website created solely to host revenge pornography was made available to the public.[157]

of stalking and harassment. Consequently, it can be argued that these figures do not truly represent the extent of harassment and stalking. See chapter four for more information.

[155] The BBC n.153

[156] HC Deb 19 June 2014, vol 582, col 1368

[157] Scott R Stroud, 'The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn' (2014) 29(3) Journal of Mass Media Ethics 168, 170

In 2015 Westminster Parliament criminalised the conduct of revenge pornography under section 33 of the Criminal Justice and Courts Act, following concerns the behaviour fell outside the criminal law.[158] Within the first year of the Act receiving Royal Assent, 206 individuals were prosecuted under section 33 of the Criminal Justice and Courts Act.[159] However, the BBC in December 2015 placed a Freedom of Information request with all forty-three police forces in England and Wales to determine the extent of revenge porn.[160] In total thirty-one forces replied, where it was found that across all thirty-one forces a total of 1,160 reports of revenge pornography were made to the police between April 2015 and December 2015. Of this, 11% of cases resulted in another being charged with the distribution of revenge pornography, 7% of defendants received a caution and in 61% of cases, no further action was taken.[161] By 2017 the total number of successful prosecutions for revenge pornography in England and Wales rose to 465.[162]

The statistics above illustrate the continued issue of revenge pornography in a digital society. Section 33 of the Criminal Justice and Courts Act was implemented both as a form of deterrence and to ensure that:

> '… those who fall victim to this type of disgusting behaviour … know that we [the criminal justice system] are on their side and will do everything we can to bring offenders to justice.'[163]

---

[158] HC Deb 19 June 2014, vol 582, col 1372
[159] The BBC, 'Revenge porn: More than 200 prosecuted under new law' *The BBC* (London, 6 September 2016) <http://www.bbc.co.uk/news/uk-37278264> accessed 12 February 2018
[160] Peter Sherlock, 'Revenge pornography victims as young as 11, investigation finds' *The BBC* (London, 27 April 2016) <http://www.bbc.co.uk/news/uk-england-36054273> accessed 12 February 2018
[161] *Ibid.,*
[162] The Crown Prosecution Service n.154, 17
[163] Chris Grayling, 'Press release: New law to tackle revenge porn' (*Gov.uk*, 12 October 2014) <https://www.gov.uk/government/news/new-law-to-tackle-revenge-porn> accessed 11 December 2017

As detailed in chapter five the criminalisation of revenge pornography is a significant step forward for society, but there continues to be issues with the current application of section 33 of the Criminal Justice and Courts Act.

The Effects of Online Abuse

Online abuse as demonstrated above can take many forms, from traditional bullying, which can now take place online, to explicit sexualised images being actively shared across social media sites. Though there is no one true definition of abuse, or in fact no study that truly reflects the extent of online abuse, it is becoming an increasing problem for schools, society and the criminal justice system. For example, the problems of cyberbullying were affirmed by the then Prime Minister Theresa May during Prime Ministers Questions on 12 December 2018:

> 'We need to address cyberbullying … this remains a serious issue for millions of people … but we [the Government] should all be taking this issue seriously and the Government will continue to work on this.'[164]

As will be discussed throughout this thesis online abuse can have detrimental effects on a person's wellbeing, alongside changing how they utilise social media, mirroring some aspects of victimology as outlined in the following chapter.

Furthermore, the Law Commission has highlighted several harms associated with online abuse:

> 'We have seen that specific harms resulting from being the recipient of abusive and offensive communication[s] online can include: (1) psychological effects and emotional harms; (2) physiological harms; including suicide and self-harm; (3) exclusion from public online space

[164] Teressa May, HC Deb 12 December 2018, vol 651, cols 277-288

> and corresponding feelings of isolation; (4) economic harms; and (5) wider societal harms.'[165]

Ben McKenzie a schoolboy from Scotland in early October 2018, committed suicide following relentless bullying online.[166] Similarly, those who become victims of revenge pornography are prone to suicidal thoughts.[167] For example, a study conducted in the United States of America found that 51% of revenge porn victims considered taking their own life.[168] These findings have also been mirrored in the work of Bates, who undertook interviews with victims of revenge pornography:

> 'The moments after you first see your naked photos on the Internet for display is a pivotal moment in your life. It's a moment when time stands still, and everything, EVERYTHING changes. In an instant you lose not only your privacy and your confidence, but you are soon made to feel you've lost your voice as you cry out for help, and it seems no one's listening [*sic*].'[169]

Bates' research which is discussed further in chapter five exposes the real-life consequences of revenge pornography. Yet for some commentators, if a person wishes not to be abused online, they should simply remove themselves from the online world,[170] reflecting aspects of positivist victimology discussed further in chapter two.

---

[165] Law Commission n.15, [3.30]
[166] HC Deb 12 December 2018, vol 651, col 276
[167] Sophia Ankel, 'Many revenge porn victims consider suicide – why aren't schools doing more to stop it?' *The Guardian* (London, 7 May 2018) <https://www.theguardian.com/lifeandstyle/2018/may/07/many-revenge-porn-victims-consider-suicide-why-arent-schools-doing-more-to-stop-it> accessed 13 December 2018
[168] *Ibid.,*
[169] Samantha Bates, '"Stripped": An Analysis of Revenge Porn Victims' Lives after Victimization' (Master of Arts Thesis, Simon Fraser University 2015) 1
[170] For instance, see, Rosalee Dorfman, 'Can you say "social media prosecutions" with a straight face? The Crown Prosecution Service can' (2013) The Leeds Journal of Law and Criminology <http://criminology.leeds.ac.uk/2013/09/05/social-media-prosecutions/> accessed 20 October 2016

A prevalent argument that is raised during discussions and reports of online abuse, is that a person can simply remove themselves from the abusive situation by shutting down their social media accounts.[171] For instance in some police forces, this is the main advice given to victims who report online abuse.[172] In fact, traditional victimology theory emphasises the victims' role in their own victimisation shown further in the work of Mendelsohn, as discussed further in the following chapter.[173] However, as is apparent above and through later chapters of this thesis, social media dominates much of society today. Thus, removing oneself from social media is to withdraw from an important aspect of social life.[174]

Consequently, those who are victims of online abuse are being blamed for the behaviour they have been subjected to, simply for having a social media profile. This victim-blaming approach is *akin* to the advice given to women when it comes to sexual violence within the physical world. For example, women who become victims of sexual assaults are often stigmatised by their choice of clothing or their decision to walk home alone in the dark. Here, we are seeing individuals now being blamed for the abuse they suffer online because they happened to have a social media profile.[175] To advise victims

---

[171] *Ibid.,*
[172] Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate, 'Living in fear – the police and CPS response to harassment and stalking' (*justiceinspectorates.gov*, July 2017) 52 <http://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/living-in-fear-the-police-and-cps-response-to-harassment-and-stalking.pdf> accessed 29 November 2017
[173] Benjamin Mendelsohn*, '*Une *nouvelle* branche de la science bio-psycho-sociale: la *victimologie' (1956) Revue internationale de criminologie et de police technique* 10-31 found in Rob Mawby & Sandra Walklate, *Critical Victimology* (Sage 1994) 12
[174] Bernal n.1, 19
[175] Laura Bliss, 'Abuse of women MPs is not just a scandal – it's a threat to democracy' *The Conversation* (London, 17 July 2017) <https://theconversation.com/abuse-of-women-mps-is-not-just-a-scandal-its-a-threat-to-democracy-80781> accessed 9 December 2018

of online abuse to remove themselves from the online world is to curtail their own right to freedom of expression. All of which has a direct effect on the victim of online abuse, as opposed to the perpetrator of such behaviour.

Chapter Overview

Since the creation of computer networks and the World Wide Web, Internet usage has been on the increase. The Internet has changed how businesses operate, has become prominent within politics and has changed how individuals communicate. Social media has been a driving force for these changes. We have seen Twitter used as a mechanism to highlight the subtle everyday sexism present within society.[176] We have also seen Facebook used as an aid to inform loved ones that a person is safe following real-world events;[177] it has, as Bernal argues become integral to the way in which society operates.[178] Yet as demonstrated above social media has a darker side whereby it can be used to abuse and torment another person, placing increasing pressure on the criminal justice system, society and social networking companies to do more.

[176] Laura Bates, 'The everyday sexism project' (*Everydaysexism*, 2019) <https://everydaysexism.com/> accessed 6 February 2019
[177] Facebook, 'Crises Response' (*Facebook*, 2019) <https://www.facebook.com/about/crisisresponse/> accessed 6 February 2019
[178] Bernal n.1, 19

Chapter Two

Theoretical Positioning: Legality in the Criminal Law

> 'The law must be open and adequately publicised. If it is to guide people, they must be able to find out what it is. For the same reason its meaning must be clear. An ambiguous, vague, obscure or imprecise law is likely to mislead or confuse at least some of those who desire to be guided by it.'[1]

One of the fundamental principles underpinning the criminal law is that of legality. The law at its very basic must be in place, open and clear for individuals to be governed by it. The following discussion will justify the theoretical positioning of this thesis: legality. To do this, two key criminological perspectives of crime prevention theory, deterrence and rational choice theory will be examined, before turning to look at feminist theory and victimology, allowing a justification to be put forward as to why the principle of legality is the perspective that underpins this thesis. It will be argued in further chapters of this thesis that the prosecution of social media offences, under the current criminal law framework, breaches the principles of legality and consequently undermines the rule of law. To fully comprehend the arguments that will take place in the following chapters, the discussion below will start by outlining how the Criminal Justice System in England and Wales works. In addition, the concepts of *actus reus* and *mens rea* will be explained, as without these two key criminal law principles, it may be considered that no criminal offence has occurred.[2]

[1]Joseph Raz, 'The Rule of Law and its Virtue' (1977) 93 Law Quarterly Review 195,198-199
[2] There are crimes which can be committed without a *mens rea* needing to be present. However, for the purpose of this thesis all crimes which are examined contain a *mens rea* element.

The Criminal Justice System and Key Terminology

The criminal justice system in England and Wales is unique compared to other jurisdictions. For criminal law proceedings to commence the complained about behaviour needs to be brought to the attention of the police. In England and Wales, there are currently 43 police forces, all of which have jurisdictional boundaries.[3] Each police force investigates crimes which have been reported within their jurisdictions, gathering evidence and witness statements before presenting the case to the Crown Prosecution Service.

Before 1986 prosecutions brought before the courts were instigated by the police force investigating the complaint.[4] However, following concerns about a lack of consistency and objectivity in recommendations for prosecution, a national Crown Prosecution Service was created, commonly referred to as the CPS.[5] The CPS is an independent body who ultimately decide which cases should be put forward for prosecution, determine the appropriate charge for an offence based on the evidence gathered by the police, and prepare a case for court.[6]

To create consistency across the criminal justice system in England and Wales the CPS also produce, with the aid of consultations, prosecuting

[3] The Crown Prosecution Service, 'The Criminal Justice System' (*CPS.gov*, 2017) <https://www.cps.gov.uk/criminal-justice-system> accessed 24 June 2019
[4] Steve Wilson, Helen Rutherford, Tony Storey & Natalie Wortley, *English Legal System* (2nd edn, Oxford University Press 2016) 56
[5] *Ibid.,* 56. See also, Prosecution of Offences Act 1985 section 1
[6] The Crown Prosecution Service, 'The Crown Prosecution Service' (*CPS.gov*, 2019) <https://www.cps.gov.uk/> accessed 24 June 2019

guidelines. These guidelines are used to help prosecutors working at the CPS in determining whether a case should be put forward for prosecution, using a two-stage approach.[7] First, the complained about behaviour must pass the evidential stage. Here, prosecutors '… must be satisfied that there is sufficient evidence to provide a realistic prospect of conviction against each suspect on each charge', using the evidence before them.[8] A matter which does not pass the evidential test, will not proceed to court. However, even if the evidential test is surpassed, it does not automatically mean the matter is worthy of prosecution, it must also pass the public interest element.[9]

The public interest test consists of a number of relevant factors a prosecutor must take into consideration before coming to a decision. For instance, the seriousness of the offence, the age and maturity of the suspect and proportionality.[10] If both these tests are passed a recommendation for prosecution will be made and the matter will be put before the courts.

Actus Reus

In most criminal law proceedings the first step is to establish the *actus reus* of the offence.[11] The *actus reus* '… comprises all the elements of the definition of the offence except those which relate to the mental element

[7] The Crown Prosecution Service, 'The Code for Crown Prosecutors' (*CPS.gov*, 26 October 2018) <https://www.cps.gov.uk/publication/code-crown-prosecutors> accessed 19 February 2019
[8] *Ibid.,*
[9] *Ibid.,*
[10] *Ibid.,*
[11] In some cases, the *mens rea* needs to be established first. For example, offences conducted under section 1 of the Prevention of Crime Act 1953.

(*mens rea*) required on part of the [defendant].'[12] Put simply, the *actus reus* is considered the criminal act itself and is either contained in the common law definition of the offence or found within an Act of Parliament. For example, under section 1 of the Protection from Harassment Act 1997 the *actus reus* is '… a course of conduct which amounts to the harassment of another …'.[13] To satisfy a breach of the *actus reus* of any offence the conduct must be voluntary: '[the] requirement that it should be a voluntary act is essential not only in a murder case, but also in every criminal case.'[14]

Mens Rea

With the exception of strict liability offences for a person to be liable for a criminal act they need to have the precise '… mental element, necessary for the crime', known as the *mens rea*.[15] Like that of the *actus reus*, the *mens rea* will either be contained in the common law or an Act of Parliament.[16] The exact mental element required to commit an offence can differ depending on the crime, examples include intention, recklessness and knowledge,[17] all of which are relevant when examining social media offences.

Intention can be split into two categories: a direct intention or an oblique intention. Direct intention referrers to '… someone's aim, purpose or

[12] Michael J Allen, *Criminal Law* (14th edn, Oxford 2017) 34
[13] The Protection from Harassment Act 1997 will be discussed in further detail in chapter four.
[14] *Bratty Appellant v Attorney-General for Northern Ireland Respondent* [1961] 3 W.L.R. 965, [1963] A.C. 386 per Lord Denning 409
[15] Allen n.12, 76
[16] The courts can also substitute a *mens rea* element into an offence following the principles of *Sweet v Parsley* [1969] 2 W.L.R. 470, [1970] A.C. 132 where the criminal act is considered a true crime as opposed to a regulatory offence.
[17] These are the main *mens rea* elements present in Acts used to prosecute social media related offences.

desire.'[18] Whereas an oblique intention is considered to occur as a result of an indirect consequence of the defendant's actions.[19] Though the overall definition of intention has been debated by the courts and the Law Commission alike, it has come to be accepted that intention refers to the virtual certainty of harm:

> 'Where the charge is murder and in the rare cases where the simple direction is not enough, the jury should be directed that they are not entitled to infer the necessary intention, unless they feel sure that death or serious bodily harm was a virtual certainty (barring some unforeseen intervention) as a result of the defendant's actions and that the defendant appreciated that such was the case.'[20]

Though the judgment above uses the example of murder to illustrate intention, the courts have come to accept that this approach applies to all criminal law offences requiring the *mens rea* of intent.[21]

A further *mens rea* element found in some communication offences is knowledge which '… involves having seen, heard or experienced something [for] yourself.'[22] For example, the *mens rea* needed to prosecute an individual for harassment is based on the construction of knowledge, whereby the defendant must 'know or ought to know' that their actions amounted to harassment.[23] In *Taylor's Central Garages (Exeter) v Roper*[24] Devlin J suggested that there was a spectrum applied by the courts when it comes to the *mens rea* of knowledge. First, there is 'actual knowledge' which

[18] Jacqueline Martin & Tony Storey, *Unlocking Criminal Law* (4th edn, Routledge 2013) 62
[19] Alan W. Norrie, 'Oblique intention and legal politics' (1989) Nov Criminal Law Review 793
[20] *Regina Respondent v Woollin Appellant* [1998] 3 W.L.R. 382, [1999] 1 A.C. 82 per Lord Steyn 93
[21] Allen n.12, 91
[22] *Ibid.,* 96. See also, *R v Abdul Sherif* [2008] EWCA Crim 2653, [2009] 2 Cr. App. R. (S.) 33
[23] Protection from Harassment Act 1997 section 1(a)
[24] *Taylor's Central Garages (Exeter) v Roper* [1951] 2 T.L.R. 284

is like that of intention.[25] The second degree of knowledge for Devlin J is 'wilful blindness', which is considered as 'closing your eyes and ears to the truth'[26] and is relevant in cases of harassment. Last, and the furthest from 'actual knowledge' is 'constructive knowledge', here it falls on the concept that the defendant should have reasonable knowledge that their behaviour caused a certain consequence.

The final *mens rea* element, which is relevant in social media related offences, is recklessness. A subjective approach is undertaken in relation to recklessness where it must be found that the defendant:

> '... is aware of a risk that it exists or will exist; [and] … is aware of a risk that it will occur; and it is, in the circumstances known to him, unreasonable to take the risk.'[27]

If these elements are found the criteria of recklessness will be satisfied. For example, under section 3 of the Computer Misuse Act 1990, it is an offence to impair the operation of a computer. Here the *mens rea* is one of recklessness or intent. Consequently, you can be prosecuted for an offence under this section of the Act even if your intention was not to impair the operation of the computer. If it can be proven that the *actus reus* and the *mens rea* are present in a matter, the main foundations are established for the possible prosecution of a criminal offence.[28]

[25] Allen n.12, 97
[26] *Ibid.,* 97
[27] *R v G and Another* [2003] UKHL 50, [2004] 1 A.C. 1034 per Lord Bingham [41]
[28] In some criminal offences other matters also need to be proven. For instance, a chain of causation.

Theoretical Stance

The following discussion will outline several theoretical theories, including, deterrence theory, rational choice theory, feminism, digital feminism and victimology, before turning to look at the principle of legality; the theoretical concept underpinning this thesis. As previously mention, legality is the concept that a person cannot be punished without clear and accessible legal provisions within a given society. Throughout the following discussions, reference will be made as to why legality forms the theoretical perspective of this thesis, as opposed to the other perspectives outlined below, allowing the researcher to justify their theoretical position.

Criminological Theory: Deterrence and Rational Choice

Criminology is the study of crime and justice, in which several different theoretical perspectives have developed, including biological and psychological causes of criminality, many of which were heavily criticised as ignoring external factors such as the criminal justice system itself.[29] The sociology of criminality will be examined in the following sections, whereby two key criminological perspectives of crime prevention theory, deterrence and rational choice theory, will be examined.

Deterrence, at is very basic, is the idea that by having strong penal sanctions this will deter individuals from either reoffending or offending in the first

[29] Katherine S. Williams, *Textbook on Criminology* (7th edn, Oxford University Press 2012) 301

place.[30] Stemming from the work of Banduara,[31] it is suggested that under certain circumstances '… punishment can effectively and efficiently control behaviour …'.[32] Geerken and Grove suggest that for deterrence to work the offender needs to know that if they commit a certain act this will be detected by the appropriate authorities and once detected the probability of being caught, convicted and punished is high, with the punishment outweighing the benefit of committing the offence.[33] This is a similar approach to Paternoster who argues that there needs to be a causal link between justice policy and the cost-benefit of committing an offence for deterrence to be successful.[34]

In a social media context, the current application of the criminal law can be seen to offer little deterrence. For instance, the most prominent provision used in a social media offence is that of section 127 of the Communications Act, which as discussed in chapter six, prohibits the use of a communications network to send a malicious, grossly offensive, obscene or indecent message, carrying a maximum 6 month custodial sentence. In reality, from a review of case law examples and the Crown Prosecution Service Guidelines, a sentence of 12 weeks is usually given, which in many cases is suspended.[35] Consequently, examples are given in the following discussion of social media 'trolls' reoffending, such as that of John Nimmo, as

[30] Richard Sparks, 'Prison, Punishment and Penality' in Eugene McLaughlin & John Muncie, *Controlling Crime* (2nd end, The Open University 2001) 204
[31] Albert Bandura, *Principles of Behavior Modification* (Holt, Rinehart and Winston 1969)
[32] Michael Geerken & Walter Grove, 'Deterrence: Some Theoretical Considerations' (1975) 9(3) Law and Society 497
[33] *Ibid.,* 499
[34] Raymond Paternoster, 'How much do we really know about criminal deterrence' (2010) 100 (3) Journal of Criminal Law and Criminology 765, 787
[35] This has been generated from a narrative review of the literature throughout this thesis. See introductory chapter for a discussion on methods and methodology.

highlighted in chapter four,[36] arguably because of a lack of deterrence in the law.

However, like that of Davis, Croall and Tyrer, the researcher accepts that a criminal justice system built purely on deterrence is in itself flawed:

> '… a deterrence approach to sentencing is an unrealistic policy because it assumes that criminals make calculations about the likelihood of being detected, arrested and punished, and mostly they do not …'.[37]

The criminal justice system needs to invoke more than deterrence, as highlighted in section 142(1) of the Criminal Justice Act 2003, in which Parliament has set out considerations the court must take into account when sentencing:

> 'Any court dealing with an offender in respect of his offence must have regard to the following purposes of sentencing (a) the punishment of offenders, (b) the reduction of crime (including its reduction by deterrence), (c) the reform and rehabilitation of offenders, (d) the protection of the public, and (e) the making of reparation by offenders to persons affected by their offences.'

Deterrence, however, remains one of many factors which underpin the criminal justice system in England and Wales.

Yet, in order for deterrence to work, the law itself needs to be clear and certain. Consequently, some of the discussions in the following chapters mirror some concepts of deterrence theory, though from the perspective of legality. As noted above, stronger legal provisions governing online conduct

---

[36] Sandra Laville, 'Internet troll who sent labour MP antisemitic abused is jailed' *The Guardian* (London, 10 February 2017) <https://www.theguardian.com/uk-news/2017/feb/10/internet-troll-who-sent-labour-mp-antisemitic-messages-is-jailed> accessed 13 January 2020

[37] Malcolm Davis, Hazel Croall & Jane Tyrer, *Criminal Justice* (4th edn, Pearson Education 2010) 417

built purely on deterrence leaves open the idea that those who conduct online abuse, make a fully conscious decision, weighing up the risks and benefits, before partaking in abusive behaviour. However, this is not always the case according to Cook, Schaafsma and Antheunis, who's study found that there are a variety of factors that influence internet trolls.[38] Consequently, the following discussions do not take a fully deterrent theoretical stance.

Whereas Davis, Croall and Tyrer argue that criminal behaviour stems from opportunity, those that endorse a rational choice theoretical approach to crime and punishment, such as Becker,[39] believe that offenders make rational choices, by using a reward benefit analysis. In essence, '[p]eople *choose* to offend in order to benefit themselves'.[40] For Williams, several factors are taken into account by the offender to determine if they should commit a certain criminal act.[41] First, the offender takes into consideration wider external factors such as the likelihood of being caught. Second, an offender is more likely to commit a crime '… in the absence of suitable guardians'[42], as demonstrated in the work of Clarke, who found that the upper deck of a bus, especially the back rows, were more likely to be vandalised due to a lack of supervision.[43] Last, how easy it was to obtain the target of the offence, for example, an offender is more likely to steal a car if

[38] Christine Cook, Juliette Schaafsma & Marjolijn Antheeunis, 'Under the bridge: an in-depth examination of online trolling in a gaming context' (2017) 20(9) New Media & Society 3323
[39] Gary Becker, 'Crime and Punishment: An Economic Approach' (1968) 76(2) Journal of Political Economy 169
[40] Williams n.29, 312
[41] *Ibid.,* 312-313
[42] *Ibid.,*
[43] Ronald Clarke, *Tackling Vandalism* (Home Office Research Study 47, 1978)

the vehicle is left unlocked. William's goes further to suggest that in order to reduce the likelihood of a person committing a criminal act, we can simply remove the target of the offence, which in turn would reduce crime rates.

This theoretical understanding of crime is somewhat mirrored when examining offences conducted by social media. As outlined in the following chapter, there is a clear lack of supervision in the online world, whereby gatekeepers such as Facebook and Twitter, are doing very little to tackle abusive behaviour online. Indeed, cuts to police funding and the criminal justice system means that in many cases the internet is becoming like the 'wild west',[44] whereby abusive and offensive behaviour can flourish. Yet to remove the target of the criminal act, i.e the victim of online abuse, this would place the onus on the victim as opposed to the perpetrator, encroaching on victim-blaming. As will be outlined in chapter seven, by asking the victim of online abuse to remove themselves from social media platforms, we are in turn, curtailing their own right to freedom of expression, whilst also punishing the victim as opposed to the person committing the offence. As discussed below, the internet has become a platform for minority voices to be heard, in particular women. Consequently, this thesis does not approach the research questions from the perspective of rational choice theory, as this theoretical position seems to place an onus on the victim changing their own behaviour to reduce criminal acts, as opposed to tackling those who commit the offence in the first place.

[44] David Omand, 'The dark net: Policing the internets underworld' (2016) Winter 2015/16 World Policy Journal <https://worldpolicy.org/2015/12/09/the-dark-net-policing-the-internets-underworld/> accessed 13 January 2020

Feminism and Digital Feminism

Feminist theory '… is a vibrant intellectual practice that raises new questions, brings new evidence, and poses significant challenges to academic discipline.' In essence, feminism is concerned with the lived experiences of women within a patriarchal society. Emerging in the late 19th century feminism formed as a rebellion against the patriarchal state, which was considered to have been built on, and maintained, the dominance of man over woman. Indeed, for Millet

> 'our society … is a patriarchy. The fact is evident at once if one recalls that the military, industry, technology, universities, science, political offices, finances- in short, every avenue of power within the society, including ... the police, is entirely in male hands.'[45]

Prior to the emergence of feminism, it was argued that the voices of women were being ignored within society:[46] 'The very creation of feminist civil society was necessary because women and women's issues have been and continue to be solely neglected by governments.'[47] Traditional positivist research therefore focused on statistical data gathered from men and universally applied to women, indeed, women were seen as 'other'.[48] For example, until 2012 women were more likely to be killed or seriously injured in a car accident than their male counterparts, as car crash dummies were built on the male physique, creating what Criado-perez refers to as the

[45] Kate Millet, *Sexual Politics (*Avon Books 1971) 25
[46] Pamela Abbott, Claire Wallace & Melissa Tyler, *An Introduction to Sociology: Feminist Perspectives* (3rd ed, Routledge 2005) 9
[47] Ki-Young Shin, 'Goverance' in Lisa Disch & Mary Hawkesworth (eds) *The Oxford Handbook of Feminist Theory* (Oxford University Press 2016) 319
[48] Simone *de Beauvoir, The Second Sex* (Vintage 1949) 16

gender data gap.[49] Feminist research studies, invoking what is deemed as feminist research methods such as interviews and stories, is therefore considered as bridging the gender gap within research and data to influence social change within society, which has a direct benefit on women.[50]

Though there are many strains of feminist theory,[51] three common characteristics emerge throughout each perspective.[52] First, indifferences such as race and sex are political concepts that pass for differences within society, built upon the ideal of the patriarchal hierarchy. Second, the need to challenge the concept that knowledge is universal and impartial. Indeed, for Geigner, 'what constitutes feminist work is a framework that challenges existing androcentric or political constructions of women's lives.'[53] Last, the need to engage with the complexity of power relations. This is evident when it comes to the use of technology and the internet, which as highlighted above by Millet is encompassed in patriarchal culture. Cockburn goes as far as arguing that men are considered as technologically 'endowed' whereas women are seen as technically 'incompetent.'[54] Consequently, we have seen the emergence of abusive and oppressive behaviour directed at women *via*

[49] Caroline Criado-perez, *Invisible Women: Exposing Data Bias in a World Designed for Men* (2019 Chatto & Windus)
[50] Although the general consensus is that qualitative methodological approaches are preferred by feminists, quantitative methods are also used in some feminist research. See, Andrea Douget & Natasha S Mauthner, 'Feminist Methodologies and Epistemology' in Clifford D Bryant & Dennis L Peck (eds), *Handbook of 21st Century Sociology* (Sage 2006)
[51] Other common feminist theoretical positions include liberal feminism, radical feminism, black feminist theory and Marxist feminists. Please note this is not a complete list.
[52] Lisa Disch & Mary Hawkesworth (eds) *The Oxford Handbook of Feminist Theory* (Oxford University Press 2016) 5
[53] Susan Geiger, 'What's So Feminist about Women's Oral History?' (1990) 2(1) Journal of Women's History 169
[54] Cynthia Cockburn, *Brothers: Male Dominance and Technological Change* (Pluto Press 1983) 159

the use of social media sites such as Facebook and Twitter, paving the way for digital feminism.[55]

Following the advancements of technology, in particular the internet, feminism has evolved to encompass the digital world, changing feminist discourse. Prior to the advancement of technology radical feminists, 'inspired by the necessity to expose the collective harms they discovered in consciousness-raising groups, to raise public consciousness and to provide political response', organised 'speak-outs' in local village halls, the streets and public spaces to tell their stories.[56] Now, the advancement of digital technology has allowed campaigns and activism to solely run online, whilst also creating a public platform for women's voices to be heard. As potently put by Powell and Henry, '[n]ever before has our society had so many publicly available, first-hand accounts of women's experiences of diverse forms and "everyday" infractions of sexual violence.'[57]

Digital feminism stems from digital criminology, which seeks to conceptualise traditional criminological, sociological and political theories in the study of crime and justice in line with the advancements in changing technology.[58] For Stratton, Powell and Cameron:

> '… criminology can account for the enabling and disabling effects of technologies … to conceptualise crime, deviance and justice as

[55] Paula Hamilton & Mary Spongberg, 'Twenty Years On: feminist histories and digital media' (2016) 26(5) Women's History Review 671
[56] Renee Heberle, 'The Personal is Political' in Lisa Disch & Mary Hawkesworth (eds) *The Oxford Handbook of Feminist Theory* (Oxford University Press 2016) 598
[57] Anastasia Powell & Nicola Henry, *Sexual Violence in a Digital Age* (Springer 2017) 26
[58] Anastasia Powell, Gregory Stratton & Robin Cameron, *Digital Criminology: Crime and Justice in Digital Society* (Routledge 2018)

increasingly *technosocial practices* within a *digital society*.'[59]

Those who endorse a digital feminist approach to their studies view digital criminology from a feminist perspective, in which Jackson argues that traditional feminist theory entwines with the digital world in three ways.[60] First, it can be used as a tool for feminist practice, which is evident in the recent use of social media to create a movement to call out the use of sexual harassment and sexual assault within society through the use of the hashtag 'metoo'. Here, using the hashtag individuals spoke publicly on platforms such as Twitter to tell their stories of sexual harassment and assault. Second, the use of digital technology allows for the sharing of knowledge as evident above, and third, as a way of doing feminist practice.[61]

Whereas traditional forms of research were criticised for ignoring the voices of women, digital feminism allows women to have a public platform for which their voices can be heard. We have seen the use of social media sites such as Facebook and Twitter used to highlight the everyday sexism that exists within society with #everydaysexism;[62] the use of social media to organise protests to challenge the '… sexism, racism and xenophobia of the Trump Administration';[63] and as a space for women to challenge stereotypical

[59] Greg Stratton, Anastasia Powell & Robin Cameron, 'Crime and Justice in Digital Society: Towards a Digital Criminology?' (2016) 6(2) International Journal for Crime, Justice and Social Democracy 17, 24
[60] Sue Jackson, 'Young Feminists, Feminism and Digital Media 2018' 28(1) Feminism & Psychology 32
[61] *Ibid.,*
[62] Laura Bates, 'The everyday sexism project' (*Everydaysexism*, 2019) <https://everydaysexism.com/> accessed 6 February 2019
[63] Kaitlynn Mendes, Jessica Ringrose & Jessalynn Keller, *Digital Feminist Activism: Girls and Women Fight Back Against Rape Culture* (Oxford University Press 2019) 4

conceptions of rape;[64] highlighting how the internet can be used as both a tool and mechanism for feminist practice, whilst also helping to distribute knowledge. However, in turn misogynistic attitudes and behaviours towards women have also emerged in an online context.

As argued in the following chapters, though anyone can become a victim of online abuse, it is apparent that women are becoming subjected to a unique form of abuse online in which threats of sexual violence are often used to curtail female discourse on social media; online abuse is subsequently becoming a feminist issue.[65] Throughout this thesis, case studies relating to abusive behaviour aimed at women are utilised to demonstrate the inadequacies in the current criminal law framework in protecting women from online abuse. References are made to traditional feminist arguments surrounding victim blaming and victim hierarchy, alongside key arguments relating to digital feminism. For instance, Karusala, Bhalla and Kumar suggest that advancing technology can be used to maintain patriarchal culture by suppressing the voices of women.[66] However, this thesis does not take a wholly feminist theoretical position, as the findings and recommendations put forward in the following discussions, can be argued to go against some of the key principles of feminism. For instance, the use of

[64] Jessamy Gleeson, '"(Not) working 9–5": the consequences of contemporary Australian-based online feminist campaigns as digital labour' (2016) 16(1) Media International Australia 77 <http://journals.sagepub.com/doi/pdf/10.1177/1329878X16664999> accessed 13 January 2020

[65] Emma A Jane, 'Online Misogyny and Feminist Digilantism' (2016) 30(3) Journal of Media and Cultural Studies 284

[66] Navenna Karusala, Apoorva Bhalla & Neha Kumah, Privacy, Patriarchy, and Participation on Social Media (2019) <https://static1.squarespace.com/static/59f549a3b7411c736b42936a/t/5cc217ed1464540001305a53/1556223981510/DIS2019.pdf> accessed 13 January 2020

the criminal law to govern online behaviour may be considered as maintaining the political and patriarchal elite:[67]

> '[The state] coercively and authoritatively constitutes the social order in the interests of men through legitimating norms, forms, relation to society and substantive policies.'[68]

Consequently, by using the theoretical position of legality, as opposed to feminism, it ensures that feminist methodology is not undermined by the recommendations put forward at the end of this thesis.

Victimology

Victimology relates to an area of study in which the researcher is concerned with the relationship between the innocent party of a crime and the offender.[69] For Kearon and Godfrey, traditionally speaking, victims of crime were ignored by the criminal justice system or considered as passive bystanders, whereby the state was concerned more with the offender and reducing crime rates, rather than listening to the voices of those who were at the centre of the criminal act.[70] This was further reflected in the judicial system, whereby Fry argued that the 'injured individual slipped out the mind of the court'.[71] Consequently, an important actor within the criminal justice system was being largely ignored and still is, to some degree, today.[72]

---

[67] Meda Chesney-Lind, 'Patriarchy, Crime, and Justice' (2006) 1(1) Feminist Criminology 6, 9
[68] Heberle n.56, 598
[69] Ezzat A Fattah, 'Victims and Victimology: The Facts and the Rhetoric' in Ezzat A Fattah (ed), *Towards a Critical Victimology* (Palgrave 1992) 29
[70] Tony Kearon & Barry S. Godfrey, 'Setting the scene: a question of history' in Sandra Walklate (ed), *Handbook of Victims and Victimology* (Routledge 2011) 17
[71] Margery Fry, *Arms of the law* (Howard League for Penal Reform by Gollancz 1951) 125
[72] For instance, the CPS can put forward a recommendation for prosecution against an individual even if the victim wishes not to press charges.

Victimology emerged as a form of research following the Second World War,[73] though during early studies emphasis was placed on how the injured party had contributed to their own victimisation, illustrated in the work of Von Hentig.[74] This theoretical position known as positivist victimology is characterised by:

> 'the identification of factors which contribute to a non-random pattern of victimisation, a focus on interpersonal crimes of violence, and a concern to identify victims which may have contributed to their own victimisation.'[75]

Positivist victimology was therefore more concerned with 'street crime' as opposed to other '… kinds of criminal victimisation like violence, rape and various forms of abuse, which more often occurred behind closed doors.'[76] As Mawby and Walklate argue, this meant that certain sectors of society were ignored in early victimological research, and more often than not, the work of positivist victimologists was used to maintain the political elite, alongside patriarchal structures.[77]

Whilst the emergence of positivist victimology allowed for victims of crime to become more involved in the criminal justice system, indeed for Karmen, positivist victimology influenced the move from 'crime prevention' to 'victimisation prevention',[78] positivist victimology also encompassed a victim-blaming orthodox. For instance, Mendelsohn conducted research based on

[73] Kearon & Godfrey n.70, 26
[74] Hans von Hentig, *The Criminal and his Victim: studies in the Sociobiology of Crime* (Yale University Press 1948)
[75] Andrew Karmen, *Crime Victims: An Introduction to Victimology* (Cengage Learning 1990) 11
[76] Rob Mawby & Sandra Walklate, *Critical Victimology* (Sage 1994) 9
[77] *Ibid.,* 9-10
[78] Karmen n.75

the culpability of a victim within their own victimisation, creating six categories of victims, from 'completely innocent', that is the ideal victim, to 'the most guilty victim'.[79] This is further reflected in the work of Fattah who suggests that early victimological studies looked at the motivational and functional aspects of the victim contributing to their own victimhood, as opposed to the offender.[80]

This concept of victim-blaming is still apparent within the criminal justice system today, particularly when examining how the criminal justice system and society have dealt with victims of online abuse. As discussed in chapter four, and throughout other chapters of this thesis, those who become subjected to online abuse, are often stigmatised for having a social media account and in some cases, are informed to simply remove themselves from the online world if they do not wish to be subjected to such abuse online. For example, as outlined in chapter four, the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate report into the Protection from Harassment Act in July 2017 uncovered examples of the police advising victims of online harassment, to simply remove themselves from the social media platform in question.[81] Mirroring rape myth assumptions as discussed further in chapter five.

---

[79] Benjamin Mendelsohn, 'Une *nouvelle* branche de la science bio-psycho-sociale: la *victimologie' (1956) Revue internationale de criminologie et de police technique* 10-31 found in Rob Mawby & Sandra Walklate, *Critical Victimology* (Sage 1994) 12

[80] Fattah n.69, 30

[81] Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate, 'Living in fear – the police and CPS response to harassment and stalking' (*justiceinspectorates.gov*, July 2017) 27<http://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/living-in-fear-the-police-and-cps-response-to-harassment-and-stalking.pdf> accessed 29 November 2017

Positivist victimology is therefore not without its faults, resulting in alternative perspectives of victimology emerging. Whereas those who take a positivist approach to victimology are concerned with street crime and the culpability of a victim, those that endorse a radical approach to victimology examine '…the role of the capitalist state in victimisation' of a person, alongside taking into consideration victims of human right violations, as opposed to street crime.[82] For radical victimologists, in order to understand the victim, we need to question the role of the state and '… the role of the law within capitalist societies in defining the social construction of both the offender and the victim.'[83] Though elements of radical victimology are present within some discussions in this thesis, i.e the idea that human right violations occur on behalf of the state who ignore online abuse, the discussion throughout this thesis is more akin to critical victimology.

Critical victimology can be seen to encompass key provisions from both positivists and radical theorists. In essence, critical victimology:

> 'combines aspects of positivism and radicalism to reconceptualise the victim; looks at experiences of individual victims and the influence of social-political powers on them; critiques the victim's construction as a "consumer' of victim services.'[84]

For Goodey, critical victimology is influenced by policy initiatives, in which it is believed that research, activism and policy should be considered together to underpin social change in the criminal justice system that respects the rights of victims within the process:[85]

---

[82] Jo Goodey, *Victims and Victimology: Research, Policy and Practice* (Pearson Education Ltd 2005) 93
[83] Mawby & Walklate n.76,13
[84] Goodey n.82, 93
[85] *Ibid.,* 94

> ‘the view of science suggested here places the academic and activist in the same critical plane. They are part of the social reality in which as knowledge actors both have the capacity to influence the processes of social change. They have much to learn from each other.’[86]

For those that endorse a feminist critical victimological approach to criminal justice, activism and academic research leads to social change, which better protects the victim and erodes the notion of victim-blaming.[87] By balancing the competing interests or ideologies of both the state and the victim, this ensures that a more victim-centred policy is produced.

Throughout the following discussions weight is placed on victims of online abuse being better protected by the criminal justice system to reflect the seriousness of this conduct. As outlined at varies points in this thesis, online abuse can have detrimental effects upon the person subjected to it, including, withdrawal from social life,[88] post-traumatic stress disorder[89] and in some cases self-harm and suicide.[90] Consequently, there are significant arguments made in the following chapters which mirror critical victimology. However, these discussions do not take a wholly victimological approach and instead, as previously mentioned and discussed in detail below, the theory underpinning this thesis is that of legality. For research to be ‘truly’ victimological based, the voices of victims need to be heard.[91] This ensures

[86] Mawby & Walklate n.76, 21-22
[87] Goodey n.82, 99
[88] Mudasir Kamal & William J. Newman, ‘Revenge Pornography: Mental Health Implications and Related Legislation’ (2016) 44(3) American Academy of Psychiatry and the Law 359, 362
[89] Samantha Bates, ‘“Stripped”: An Analysis of Revenge Porn Victims’ Lives after Victimization’ (Master of Arts Thesis, Simon Fraser University 2015) 24
[90] Ann John *et al*, ‘Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review’ (2018) 20 (4) Journal of Medical Internet Research 129
[91] Goodey n.82, 117

that ‘patronising assumptions abound that victim services or the police “know best” when it comes to the state of mind and the role that crime victims play in criminal justice’ are avoided.[92] Indeed, the ‘roles of victim and victimizer are neither static, assigned nor immutable.’[93]

The Criminal Law and Legality

At its very basic the principle of legality is defined as ‘no crime without law’[94] and is considered a fundamental principle of natural justice.[95] It comprises of the logic that individuals should be able to partake in any activities knowing whether their behaviour breaches the law. Legality is supported in both national and international legal systems, with the principle having specific protection under Article 7 of the European Convention on Human Rights and Fundamental Freedoms (the Convention):

> ‘The guarantee enshrined in Article 7, which is an essential element of the rule of law, occupies a prominent place in the Convention system of protection … It should be construed and applied, as follows from its object and purpose, in such a way as to provide effective safeguards against arbitrary prosecution, conviction and punishment.’[96]

Under the Convention, Article 7 is an absolute right meaning that States who are party to the Convention cannot delegate from this right, even in times of

[92] *Ibid.,*
[93] Fattah n.69, 7
[94] Judge Theodor Meron, *The Principle of Legality in International Criminal Law* (Legal Studies Research Papers Series 10-08, 2010) 7
[95] David Luban, ‘Fairness to rightness: Jurisdiction, Legality, and the Legitimacy of International Criminal Law’ in Samantha Besson & John Tasioulas (eds), *The Philosophy of International Law* (Oxford University Press 2010) 34
[96] *Kafkaris v Cyprus* App no 21906/04 (ECtHR, 12 February 2008) [137]

national emergency.[97] Legality therefore creates certainty within the law and is described by Murphy as the '… hidden jewel of the Convention.'[98]

Luban argues that two key rationales uphold the principle of legality in the criminal law: the action-guiding character of the law and the insurance that the state will not abuse its powers.[99] The action-guiding argument stems from the philosophical work of Fuller who suggests that the law allows individuals to govern their behaviour in accordance with clear and distinct rules. Those who break these rules are subject to punishment. Nonetheless, those who break rules which are unclear and consequently are incapable of guiding those living in a society, should not be subject to punishment.[100] Luban refers to this as 'the fair notice argument'. Here, a person must be seen to have been given 'constructive notice' that their actions have breached the law.[101] For this to occur the law must be accessible and clear.

The second rationale concerns the abuse of power. In the past imprecise and flexible legislation was used by States to target oppressed groups in a given society. This is clear when examining laws enacted during Nazi Germany, which were used to target certain groups of individuals. The purpose of legality is to safeguard '… against arbitrary punishment by governments under a cover of vague, underspecified law.'[102] It creates

[97] Cian C. Murphy, 'The principle of legality in criminal law under the European Convention on Human Rights' (2010) 2 European Human Rights Law Review 192, 207. See chapter seven for an in-depth discussion of the types of rights contained within the Convention.
[98] *Ibid.,* 206
[99] Luban n.95, 37
[100] Lon L Fuller, *The morality of law* (Yale University Press 1964)
[101] Luban, n.95, 40
[102] *Ibid.,* 37

fairness within the law whilst also ensuring that States adhere to the separation of powers. The separation of powers is the idea that each body of the State, for instance the executive, the legislature and the judiciary, should be segregated and neither body should do the work of another. Though in the United Kingdom there is not a complete separation of powers, its breaches are considered lawful as it allows for checks and balances to occur between different parts of the state.[103] Therefore, the principle of legality prohibits retrospective law, maintains procedural fairness and creates clear distinct legal rules for a given society to adhere to.

From an International Criminal Law perspective, a strict approach is maintained with legality. International Criminal Law is, at its very basic, the application of criminal law across borders.[104] It is considered that there are three bodies of International Criminal Law, all of which uphold the principle of legality: domestic criminal law which is applied on an international scale; treaty-based criminal law (this is the creation of treaties between States which criminalises particular conduct); and pure international criminal law which includes crimes such as genocide, aggressive war and crimes against humanity.[105] Each source of International Criminal Law must be publicly accessible, clear and beyond doubt.[106] For international criminal law

[103] Roger Masterman, *The Separation of Powers in the Contemporary Constitution: Judicial Competence and Independence in the United Kingdom* (Cambridge University Press 2010) 24
[104] Douglas Guilfoyle, *International Criminal Law* (Oxford University Press 2016) 3
[105] Luban n.95, 19
[106] Darryl Robinson, *The Principle of Legality in International Criminal Law* (Legal Studies Research Papers Series 10-08, 2010) 4

theorists, the law must be constructed rigorously to conform to the principle of legality, as affirmed in *Čelebići*.[107]

However, strict construction of the law is not always achievable, as society changes the law needs to be adaptable, as affirmed in *R v Rimmington*.[108] Rimmington sent numerous letters and parcels containing racially offensive material. In total he sent 538 separate articles, all of which were of a racist nature. At Southwark Crown Court he was convicted under the common law offence of public nuisance, but this was quashed by the House of Lords as it was held that his actions had not affected a significant proportion of society, the mischief behind the common law offence of public nuisance. During the hearing the House of Lords examined the principle of legality, with Lord Bingham stating that there are two guiding principles:

> '… no one should be punished under a law unless it is sufficiently clear and certain … and no one should be punished for any act which was not clearly and ascertainably punishable when the act was done.'[109]

Like that of International Criminal Law theorists, Lord Bingham supports the concept that the law needs to be clear and certain, but he also maintains that absolute certainty cannot, and will not, always be desirable:

> 'It is accepted that absolute certainty is unattainable, and might entail excessive rigidity since the law must be able to keep pace with changing circumstances, some degree of vagueness is inevitable …'.[110]

---

[107] *Čelebići Camp, Prosecutor v Delalić (Zejnil) and others,* Appeal Judgment, Case No IT-96-21-A, ICL 96 (ICTY 2001), 20th February 2001, United Nations Security Council [UNSC]; International Criminal Tribunal for the Former Yugoslavia [ICTY]; Appeals Chamber
[108] *R v Rimmington, R v Goldstein* [2005] UKHL 63, [2006] 1 A.C. 459
[109] *Ibid.,* [33]
[110] *Ibid.,* [35]

The law needs to be adaptable to reflect the fast-changing nature of society; this is especially true with technology. Technology and the Internet have evolved at a significant pace and in some instances the law has struggled to keep track, as confirmed by the Law Commission in their report examining offensive commentary online.[111] The law needs to maintain some form of openness to resolve legal disputes, but this should not be at the detriment of breaching the principles of legality.

As previously stated, the principle of legality is a guaranteed right under Article 7, no punishment without law, of the Convention:

> 'No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed ...'.

Article 7 consists of two key principles: *nullum crimen sine lege* (no crime without law) and *nulla poena sine lege* (no punishment without law).[112] Similar to the International Criminal Law perspective, Schaack argues that legality helps maintain the separation of powers.[113] However, the European Court of Human Rights favours '… a broad, liberal and progressive interpretations … to give "maximum effect" to the provisions.'[114]

For Murphy the principle of legality in the Convention consists of three interrelated rules: only the law can define a crime and prescribe a penalty,

---

[111] Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018) [10.76]
[112] Susana Sanz-Caballero, 'The principle of nulla poena sine lege revisited: the retrospective application of criminal law in the eyes of the European Court of Human Rights' (2017) 28(3) European Journal of International Law 787, 788
[113] Beth Van Schaack, *The Principle of Legality in International Criminal Law* (Legal Studies Research Papers Series 10-08, 2010) 1
[114] Robinson n.106, 5

the prohibition of retrospective criminal law, and no harsher penalties can be given then those that are prescribed in the law at the time the offence was committed. The first rule was restated and affirmed in *Kafkaris v Cyprus*,[115] where the court upheld the concept that only the law can define a crime, affirming that the 'law' consists of both Acts of Parliament and the common law.[116] However, it could be suggested that pure clarity with the law encompasses aspects of rational choice theory, which as discussed above implies that individuals make a conscious decision before committing an offence, which may not necessarily be true.

The jurisprudence of Strasbourg, like that of the International Criminal Court, maintains that in order for laws, whether that be legislation or the common law, to adhere to the principle of legality it must be accessible and foreseeable. Accessibility in its simplest terms, means 'clarity', with the courts noting:

> 'An individual must know from the wording of the relevant provision and, if need be, with the assistance of the courts' interpretation of it, what acts and omissions will make him criminally liable and what penalty will be imposed … a law may still satisfy the requirement … where the person concerned has to take appropriate legal advice to assess, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.'[117]

The clarity of the law will be for the courts to decide with an emphasis being placed on the individual's knowledge that their behaviour in question 'ran a real risk of prosecution',[118] reflecting aspects of deterrence theory as discussed above. Ignorance is not a defence in law with the courts taking a

[115] *Kafkaris* n.96
[116] *Sunday Times v. United Kingdom* (no.1) App no 6538/74 (ECtHR, 26 April 1979)
[117] *Kafkaris* n.96, [140]
[118] *Cantoni v. France* App no 17862/91 (ECtHR, 15 November 1996)

firm approach to those who 'skate on thin ice' with the law: 'those who skate on thin ice can hardly expect to find a sign which will denote the precise spot where they may fall in.'[119] The rationale behind this approach surrounds the idea that citizens should know when their behaviour is unlawful, and therefore subject to punishment.[120] Though this may be true, it does not clarify which Act of Parliament an individual will be prosecuted under. When it comes to social media related offences, from an examination of case law examples discussed in later chapters, it is not always clear why a defendant was prosecuted under a particular Act. The lack of clarity exposed in these cases brings into question the principle of legality.

Like 'law', 'penalty' has also been defined by the European Court of Human Rights:

> 'The concept of "penalty" in Article 7(1) is, like the notions of "civil rights and obligations" and "criminal charge" in Article 6(1), an autonomous Convention concept. To render the protection offered by Article 7 effective, the Court must remain free to go behind appearances and assess for itself whether a particular measure amounts in substance to a "penalty" within the meaning of this provision.'[121]

Here, the principle of legality upholds the concept that an individual can only be punished to the extent to which is prescribed by law. Though this protects against arbitrary punishments, it does not protect individuals from being prosecuted under more substantial laws, if their conduct can be adapted to fit the a*ctus reus* and *mens rea* of the offence, as seen during the prosecution

[119] *Knuller (Publishing, Printing and Promotions) Ltd. and Others Appellants v Director of Public Prosecutions Respondent* [1972] 3 W.L.R. 143, [1973] A.C. 435 per Lord Morris 463
[120] Andrew Ashworth & Jeremy Horder, *Principles of Criminal Law* (7th edn, Oxford University Press 2013) 62
[121] *Welch v United Kingdom* App no 17440/90 (ECtHR, 9 February 1995) 247

of individuals following the 2011 riots in the United Kingdom. As will be explained in more detail in chapter four, riots took place across the UK in August 2011 following the death of Mark Duggan by armed police. After the riots, the then Prime Minister David Cameron spoke openly about how those who took part in criminal behaviour during the disorder would feel the full force of the law.[122] Consequently, criticism was expressed against the criminal justice system for imposing severe sentences and harsher punishments on individuals who committed criminal acts during the riots.[123] In one case a man was given a custodial sentence of four years contrary to the Serious Crime Act 2007, for the creation of a Facebook event page to incite others to participate in the riots.[124]

In addition to accessibility, the law also needs to be foreseeable. The European Court of Human Rights treats foreseeability as the concept that where there are changes in the law, these changes need to be predictable, as demonstrated in *SW and CR v United Kingdom.*[125] The defendants, who were both convicted of a similar crime but in different cases, had previously been found guilty of rape. During the trial, their defence team argued that they could not be found guilty of rape because they had committed the offence against their wives and thus, during the marriage ceremony their

[122] Andrew Sparrow, 'David Cameron announces recall of parliament over riots' *The Guardian* (London, 9 August 2011) <https://www.theguardian.com/uk/2011/aug/09/david-cameron-announces-recall-parliament> accessed 18 January 2018
[123] Andy McSmith, 'Tough riot sentences prompt new guidelines for the courts' *The Independent* (London, 17 August 2011) <http://www.independent.co.uk/news/uk/crime/tough-riot-sentences-prompt-new-guidelines-for-the-courts-2339699.html> accessed 20 January 2018
[124] *R v Jordan Blackshaw* Chester Crown Court 16 August 2011 (unreported)
[125] *SW v United Kingdom, CR v United Kingdom* App no 20166/92 (ECtHR, 22 November 1995)

wives had forever consented to sexual activity.[126] This argument was rejected by the court, and the law was extended to cover rape against a spouse.

Following their conviction, both legal teams applied to the European Court of Human Rights suggesting that Article 7 of the Convention had been breached: no punishment without law. The foundation for their argument surrounded the concept that it was not foreseeable that the law would be extended to criminalise the conduct of rape against a spouse. However, the European Court of Human Rights rejected this argument, holding that the House of Lords opinion:

> '… did no more than continue a perceptible line of case law development dismantling the immunity of a husband from prosecution for rape upon his wife. There was no doubt under the law as it stood on 18 September 1990 that a husband who forcibly had sexual intercourse with his wife could, in various circumstances, be found guilty of rape.'[127]

The court accepts the notion that the law must adapt to the changing nature of society, but this must be in a predictable manner, so citizens can guide their behaviour according to law, similar to that of rational choice theory.

Like that of accessibility, foreseeability does not extend to include certainty as to what law a defendant will be prosecuted under where there are several provisions available. For instance, if a person in England commits criminal damage, with the exception of arson, they will be prosecuted under section 1(1) of the Criminal Damage Act 1971. If their actions endanger another's

[126] It had previously been suggested under English Common Law that a husband could not be guilty of rape against his wife.
[127] *SW v United Kingdom* n.125, 402

life, they will be prosecuted under the same statute, but for a breach of section 1(2) of the Act. When it comes to abuse conducted online, it is not easy to foresee which Act of Parliament a person will be regarded as breaching. In England and Wales, a variety of provisions are used to govern online behaviour including, though not limited to, the Malicious Communications Act 1988 and the Protection from Harassment Act 1997, alongside section 127 of the Communications Act 2003. It will be exposed in later discussions that there is a lack of consistency in online abuse prosecutions, resulting in the law not being 'foreseeable'.

As the United Kingdom is a signatory to the Convention, the UK Government must comply with Article 7. Following the enactment of the Human Rights Act 1998, Article 7 can now be invoked in the national courts of the United Kingdom against state bodies. Consequently, the courts are under a legal obligation to take into consideration human rights when deciding on a legal dispute, this includes the concept of 'no punishment without law.'[128]

The principle of legality underpins the legal system of the United Kingdom and is often referred to as the rule of law:

> 'The rule of law may be interpreted either as a philosophy or political theory which lays down fundamental requirements for law, or as a procedural device by which those with power rule under the law. The essence of the rule of law is that of the sovereignty or supremacy of law over man. The rule of law incites that every person - irrespective of rank and status in society - be subjected to the law.'[129]

[128] The Human Rights Act 1988 section 6
[129] Hilaire Barnett, *Constitutional & Administrative Law* (5th edn, Cavendish Publishing 2004) 69

The rule of law constitutes several key principles depending on the philosophical-theoretical approach of the scholar, though there are some overlaps between academics understanding of these principles. For Raz, '[t]he law should conform to standards designed to guide action',[130] which among other things, means that 'all laws should be prospective, open and clear'.[131] This is a very similar approach to Fuller, as discussed previously.

The law should be action-guiding allowing citizens to conform or disregard the law at their own free will. Here, the law needs to be clear for individuals to fully comprehend when their behaviour breaches acceptable conduct in a given society. With technology-based offences this is not always clear. For instance, a breach of section 127(1) of the Communications Act 2003 occurs during the sending of grossly offensive messages. The term 'grossly offensive' is not clearly defined in the statute and the courts have concluded that it will take '… its ordinary English meaning', discussed further in chapter six.[132]

Raz's position on what constitutes the rule of law is comparable to Lord Bingham, who similarly argues that there are eight key principles which underpin the rule of law.[133] For Lord Bingham, one of the criteria for a legal rule to uphold the rule of law is that it '… must be accessible and so far as possible intelligible, clear and predictable',[134] criteria reflected both in the

[130] Joseph Raz, *The Authority of Law* (Oxford University Press 1979) 218
[131] Raz n.1, 214
[132] *Connolly v DPP* [2007] EWHC 237 (Admin), [2008] 1 W.L.R. 276 per Lord Justice Dyson [10]
[133] Lord Bingham, 'The rule of law' (2007) 66(1) Cambridge Law Journal 67
[134] *Ibid.,* 69

European Court of Human Rights and in International Criminal Law. Whereas Murray goes further stating that '… the law should be stable and certain.'[135] The current legal framework used to prosecute social media related offences can be considered uncertain and as a result, lacks stability. The variety of Acts available means there are inconsistencies in policing and prosecutions, all of which undermine the key principles of legality in the criminal law, as discussed further in the following chapters.

Rationale

Though as discussed above other theoretical positions could have been utilised to answer the research questions posed, the concept of legality was chosen as it can be considered the foundation of any criminal justice system. Without, it leaves open two possibilities, the law can be used in an arbitrary manner, as exposed further in chapter four in the case to *R v Blackshaw*,[136] or indeed it can create misunderstandings in the law, in which victims are not fully compensated for the harm that is inflicted upon them. In essence, it will be argued in the following chapters that the use of some Acts, which were in many cases never intended to cover technology, is a fundamental breach of the principle of legality in the criminal law. Before this, a discussion on social media gatekeepers will take place.

[135] Andrew D Murray, 'Mapping the rule of law for the internet' in David Mangan & Lorna E Gillies (eds), *The Legal Challenges of Social Media* (Edward Elgar Publishing 2017) 27
[136] *R v Blackshaw* [2011] EWCA Crim 2312, [2012] 1 W.L.R. 1126

Chapter Three

Social Media Gatekeepers

> 'There was literally nothing enjoyable about the job [Facebook content moderator]. You'd go into work at 9am every morning, turn on your computer and watch someone have their head cut off. Every day, every minute, that's what you see. Heads being cut off.'[1]

In recent years social media companies such as Facebook and Twitter, have come under increasing pressure to tackle inappropriate behaviour on their sites including terrorist propaganda, hate speech and revenge pornography.[2] In fact, both companies have been brought before Parliamentary Committees to explain unlawful behaviour that continues to be a problem on their sites.[3]

The following discussion will examine in detail how both Facebook and Twitter are attempting to tackle the growing issue of online abuse.[4] It will take the format of outlining Facebook and Twitter's user agreements, examining how the two companies govern hate speech, bullying, credible threats of violence and revenge pornography on their sites. The final part of this chapter will critically review some of the mechanisms Facebook and Twitter have implemented in recent years to tackle inappropriate behaviour online.

---

[1] Olivia Solon, 'Underpaid and overburdened: the life of a Facebook moderator' *The Guardian* (London, 25 May 2017) <https://www.theguardian.com/news/2017/may/25/facebook-moderator-underpaid-overburdened-extreme-content> accessed 14 January 2019

[2] Nick Hopkins & Julia Carrie Wong, 'Has Facebook become a forum for misogyny and racism?' *The Guardian* (London, 21 May 2017) <https://www.theguardian.com/news/2017/may/21/has-facebook-become-forum-misogyny-racism> accessed 14 January 2019

[3] For example, Facebook, Twitter and YouTube were brought before the Communications Committee in 2014. See, Communications Committee*, Social Media and Criminal Offences* (HL 2014-15, 37)

[4] As outlined in chapter one the focus of this thesis is on Facebook and Twitter as they are two of the biggest social networking companies today. In addition, both companies have spoken publicly about how they are continuing to tackle unlawful behaviour online.

Terms of Service Agreements

As explored in chapter one, social media companies can now be considered as part of mainstream society. As will be discussed throughout this thesis there is a darker side to social media, online abuse. This has resulted in social media companies coming under heavy criticism with how they currently attempt to eliminate this behaviour online:

> 'Social media companies are highly secretive about the number of staff and the level of resources that they devote to monitoring and removing inappropriate content.'[5]

For Bernal, social media sites are ultimately businesses where individual's rights are not always considered a priority.[6]

Due to the continued failure of both Facebook and Twitter in removing unacceptable content online, both companies have come under pressure to work quickly to get ahead of this growing problem around the world.[7] Each company has a terms of service agreement between itself and its users and is often the document quoted when they are asked to explain the decision not to remove, or in some cases remove certain content. Yet both companies acknowledge that more needs to be done to strengthen their terms of service agreements.[8]

---

[5] Hopkins & Wong n.2
[6] Paul Bernal, *The Internet, Warts and All: Free Speech, Privacy and Truth* (Cambridge University Press 2018) 49
[7] Home Affairs Committee, *Hate crime: abuse, hate and extremism online* (HC 2016-17, 609) 52
[8] *Ibid.,* 39

All social media companies have terms of service agreements, or community guidelines between themselves and their users.[9] These guidelines outline what behaviour is acceptable and unacceptable on their sites, though their content can differ dramatically between companies. All users of the site must agree to the terms of service, failure to comply can result in content being removed, suspensions and in some cases permanent exclusion from the site. The following discussion will outline and discuss the terms of services for Facebook and Twitter.

Community Guidelines: Facebook

The most recent statistics suggest that over 1.4 million people use Facebook each day.[10] Consequently, the content created, shared and liked on the site is enormous. Yet Mark Zuckerberg the CEO and founder of Facebook maintains that hate speech, bullying and terrorist material is prohibited on its site.[11] Though, he accepts that the company has 'made mistakes' in not removing such content quick enough.[12] What is and what is not allowed to be published on Facebook, is set out in its community guidelines which are built on several fundamental key principles: safety, voice and equity.[13]

---

[9] Gabriel Weimann, 'Why do terrorists migrate to social media?' in Anne Aly, Stuart Macdonald, Lee Jarvis & Thomas Chen (eds), *Violent Extremism Online: New Perspectives on Terrorism and the Internet* (Routledge 2016) 60

[10] Guardian News, 'Mark Zuckerberg testifies before Congress' (*YouTube,* 10 April 2018) <https://www.youtube.com/watch?v=mZaec_mlq9M> accessed 14 January 2019

[11] PBS NewsHour, 'Facebook CEO Mark Zuckerberg testifies before the European Union Parliament' (*YouTube*, 22 May 2018) <https://www.youtube.com/watch?v=Y70LrlzrkNk> accessed 14 January 2019

[12] Guardian News n.10

[13] Facebook, 'Community Standards: Introduction' (*Facebook*, 2019) <https://www.facebook.com/communitystandards/> accessed 14 January 2019

The community guidelines cover a range of topics including, but not limited to, hate speech, credible threats of violence, revenge pornography and bullying. Until 2017 it was not known how Facebook applied its community guidelines to its site. Following a leak by an internal source at Facebook the Guardian newspaper, based in the United Kingdom, published Facebook's moderator manuals, which for the first time gave details as to how the company comes to a decision regarding objectionable content on its site.[14]

Facebook and Hate Speech

Hate speech is defined by Facebook as:

> '… a direct attack on people based on … race, ethnicity, national origin, religious affiliation, sexual orientation, caste, sex, gender, gender identity and serious disease or disability.'[15]

Content which falls within the definition above is prohibited on its site. For instance, comments such as '[I] fuckin [*sic*] hate Christians' and 'using my freedom of speech to inform that I find homosexuals DISGUSTING [*sic*]', will be removed from the site.[16] Whereas commentary which can be labelled as targeting 'concepts, institutions and beliefs' will not be considered as breaching Facebook's hate speech policies. For example, a comment stating 'I hate Christianity' would not be labelled as hate speech.[17] Facebook maintains that in order to protect freedom of expression only conduct that falls within their definition of hate speech as given above, which is aimed at

[14] The Guardian 'Facebook Files' (*The Guardian*, 2019) <https://www.theguardian.com/news/series/facebook-files> accessed 14 January 2019
[15] Facebook, 'Community Standards: Hate Speech' (*Facebook*, 2018) <https://www.facebook.com/communitystandards/hate_speech> accessed 9 December 2018
[16] The Guardian, 'Hate speech and anti-migrant posts: Facebook's rules' *The Guardian* (London, 24 May 2017) <https://www.theguardian.com/news/gallery/2017/may/24/hate-speech-and-anti-migrant-posts-facebooks-rules> accessed 23 January 2019
[17] *Ibid.,*

individuals, groups or humans will be removed.[18] Therefore, behaviour which targets a person because of their social class, appearance or political ideology will not be considered as hate speech.[19]

On average around 66,000 pieces of content are removed each week from Facebook for violating hate speech guidelines.[20] During discussions before the European Parliament in 2018, Mark Zuckerberg emphasised the prohibition of hate speech on Facebook.[21] However, moderator guidance, published by the Guardian newspaper, exposed examples of hate speech which were considered not to breach Facebook's community standards. For instance, only recently has Facebook banned images and comments mocking those with disabilities, such as individuals with Down's Syndrome.[22] Whilst on the other hand, a picture of an abusive letter sent to Shaun King, a prominent African-American activist, published to highlight the abuse he was receiving, was removed by Facebook for breaching hate speech guidelines.[23]

Facebook has acknowledged that it has a 'long way' to go before it can be said that hate speech on its site is under control.[24] Despite this, Facebook

[18] *Ibid.,*
[19] *Ibid.,*
[20] Mark Zuckerberg, 'Building Global Community' (*Facebook*, 16 February 2017) <https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/> accessed 14 January 2019
[21] PBS NewsHour n.11
[22] Nick Hopkins, 'How Facebook allows users to post footage of children being bullied' *The Guardian* (London, 22 May 2017) <https://www.theguardian.com/news/2017/may/22/how-facebook-allows-users-to-post-footage-of-children-being-bullied> accessed 14 January 2019
[23] Sam Levin, 'Facebook temporarily blocks Black Lives Matter activist after he posts racist email' *The Guardian* (London, 12 September 2016) <https://www.theguardian.com/technology/2016/sep/12/facebook-blocks-shaun-king-black-lives-matter> accessed 14 January 2019
[24] PBS NewsHour n.11

maintains that there will always be issues with removing some content as language adapts with time.[25] For instance, what may be considered as an offensive term today, may not be in 10 years' time. Furthermore, as Facebook is available worldwide, there can be a language barrier between the user and the person moderating the content, discussed in detail in later parts of this chapter.[26]

Facebook and Bullying

Like that of hate speech, bullying is not permitted on Facebook.[27] Facebook defines bullying as conduct that shames or degrades a person which upsets or silences the individual.[28] As mentioned previously bullying is often associated with the younger generation, and Facebook is no exception. Here, the company has specific protections for minors (those under 18). For instance, posts aimed at minors which contains swearing, sexual content or negative character references will be removed, but this protection is not given to adults.[29] For example, the comment 'blondes are stupid' would not be removed if it was aimed at a person over the age of 18, as negative character references are not prohibited when directed at adults.[30] Though if the comment was aimed at a minor, the person sending the message would be in breach of Facebook's community standards. Consequently, better protection is given to minors when it comes to bullying.

---

[25] Guardian News n.10
[26] *Ibid.,*
[27] Facebook, 'Community Standards: Bullying' (*Facebook*, 2018) <https://www.facebook.com/communitystandards/bullying> accessed 3 January 2019
[28] *Ibid.,*
[29] *Ibid.,*
[30] The Guardian n.16

Whereas public figures, who Facebook defines as those with over 100,000 followers or friends, are given the least protection.[31] Here, for Facebook individuals who place themselves in the public domain should be tolerant of abuse online, with the company stating: '[W]e want to exclude certain people who are famous or controversial in their own right and don't [*sic*] deserve our protection.'[32] Encompassing aspects of Mendelsohn's theory relating to the ideal victim as discussed in the previous chapter.[33] Consequently, MPs, who during the 2017 General Election in the United Kingdom were subjected to a crusade of online abuse,[34] may not necessarily be protected by Facebook. By having a higher threshold for public figures individuals may be discouraged from placing themselves in the public domain, which in turn restricts a person's right to free speech. An issue highlighted further in chapter seven.

A strong stance against cyberbullying is needed on social media sites, as those who have been subjected to this form of abuse, have in some instances taken their own life. Facebook has therefore set a precedent for other social networking sites, but it falls short of protecting adults who are trolled online. Instead, those aged over 18 would need to rely on the

[31] Hopkins n.22
[32] *Ibid.,*
[33] Benjamin Mendelsohn*, '*Une *nouvelle* branche de la science bio-psycho-sociale: la *victimologie' (1956) Revue internationale de criminologie et de police technique* 10-31 found in Rob Mawby & Sandra Walklate, *Critical Victimology* (Sage 1994) 12
[34] Sarah Marsh, 'Surge in crimes against MPs sparks fears over intimidation and abuse' *The Guardian* (London, 23 October 2018) <https://www.theguardian.com/politics/2018/oct/23/crimes-mps-uk-online-intimidation-abuse> accessed 4 February 2019

standards of other prohibited behaviours on Facebook, for instance, credible threats of violence.

Facebook and Credible Threats

In order to breach Facebook's community standards, it must be found that a credible threat would result in 'real-world harm' before it will be deemed as inappropriate.[35] Throughout the guidelines, and during Mark Zuckerberg's testament before Congress, significant weight was given to the term 'real world harm', yet a definitive definition of this term cannot be found. In addition, the content needs to be considered as credible. For Facebook credibility is dependent on whether the content contains a specific target, there is mention of a weapon or if a location and time are present.[36] For instance, 'I'll slit your throat and hang your bloody neck by your weaves' is prohibited on the site.[37]

Like that of bullying, different criterions of protection are given to certain groups of individuals. For example, groups or individuals who are considered as 'vulnerable', have higher protection than other users.[38] Vulnerable individuals or groups include, though not limited to, Heads of States and the Pope.[39] Consequently, a comment such as 'someone shoot Donald Trump [President of the United States]' was prohibited, but a comment stating 'to

[35] Facebook, 'Community Standards: Credible Violence' (*Facebook*, 2018) <https://www.facebook.com/communitystandards/credible_violence> accessed 3 January 2019
[36] The Guardian, 'Facebook's manual on credible threats of violence' *The Guardian* (London, 21 May 2017) <https://www.theguardian.com/news/gallery/2017/may/21/facebooks-manual-on-credible-threats-of-violence> accessed 3 January 2019
[37] *Ibid.,*
[38] *Ibid.,*
[39] *Ibid.,*

snap a bitch's neck, make sure you apply all the pressure to the middle of the throat' was allowed to remain on the site.[40]

It can be suggested that a comment such as 'someone shoot Donald Trump' is closer to satire humour than a credible threat of violence, yet this comment was actively removed by Facebook. Threats evidently remain on Facebook with the Guardian newspaper exposing just some examples of comments which remained on the site, despite being reported by users as breaching Facebook's community standards:

> '"Little girl needs to keep to herself before daddy breaks her face [*sic*]" … "You arseholes better pray to God that I keep my mind intact because if I lose it I will literally kill HUNDREDS [*sic*] of you" … "Unless you stop bitching I'll have to cut your tongue out [*sic*]"'.[41]

Consequently, there remains several issues in how Facebook's community standards are used in cases of credible threats of violence on its site.

Facebook and Revenge Porn

As will be explored in chapter five revenge pornography is a growing issue in a digital age. In fact, in one month alone Facebook removed 54,000 potential cases of revenge porn.[42] Though many countries are now legislating against revenge porn, Facebook has its own rules when it comes to the removal of such content on its site. In general content that contains:

---

[40] *Ibid.,*

[41] Nick Hopkins, 'Revealed: Facebook's internal rulebook on sex, terrorism and violence' *The Guardian* (London, 21 May 2017) <https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence> accessed 21 January 2019

[42] Nick Hopkins & Olivia Solon, 'Facebook flooded with "sextortion" and "revenge porn", files reveal' *The Guardian* (London, 22 May 2017) <https://www.theguardian.com/news/2017/may/22/facebook-flooded-with-sextortion-and-revenge-porn-files-reveal> accessed 14 January 2019

> '[v]isible genitalia except in the context of birth giving and after-birth moments or health-related situations … Visible anus and/or fully nude close-ups of buttocks unless photoshopped on a public figure … Uncovered female nipples except in the context of breastfeeding, birth giving and after-birth moments, health-related situations [or] Sexual intercourse [is prohibited]'.[43]

However, as will be discussed in later chapters revenge pornography can take many forms, such as photoshopped imagery.

For Facebook, revenge pornography will only be removed when three criterions are met.[44] First, the image or video must be taken in a private place. So, for instance a photo taken on a public beach, would not fall within this criterion, and consequently it may not be removed by the company. Second, the person in the photo or video must be nude or near-nude. The term near-nude covers situations whereby a person maybe in their underwear or a costume. Last, a lack of consent must be established either through commentary on the content or by a caption. If one or more of these criterions are missing, for Facebook the content may not fall under their revenge porn policies.[45]

Summary

Throughout Mark Zuckerberg's testament before Congress and the European Parliament, he accepted that his company had made mistakes in the removal of content from its site, by allowing content that clearly breached

[43] Facebook, 'Community Standards: Adult nudity and sexual activity' (*Facebook*, 2018) <https://www.facebook.com/communitystandards/adult_nudity_sexual_activity> accessed 3 January 2019
[44] The Guardian, 'What Facebook says on "sextortion" and "revenge porn"' *The Guardian* (London, 22 May 2017) <https://www.theguardian.com/news/gallery/2017/may/22/what-facebook-says-on-sextortion-and-revenge-porn> accessed 3 January 2019
[45] *Ibid.,*

the company's terms of service agreement to remain publicly viewable. What Facebook is doing to try and reduce unacceptable behaviour on its site, will be examined in later parts of this chapter. The following discussion will outline Twitter's terms of service agreement.

Terms of Service: The Twitter Rules

When Twitter first launched in 2006, 244 tweets were sent on its first day. Five years later users sent 244 tweets in less than a tenth-of-a-second.[46] It is currently estimated that over 500 million tweets are sent every day on Twitter.[47] Similarly, like that of Facebook, Twitter continues to have issues with hate speech, bullying, credible threats of violence and revenge pornography on its site, as highlighted by Twitter's Chief Executive: '[W]e see voices being silenced on Twitter every day. We've been working to counteract this for the past 2 years.'[48] Yet the company maintains that Twitter:

> '… is reflective of real conversations happening in the world and that sometimes includes perspectives that may be offensive, controversial, and/or bigoted.'[49]

Content that is prohibited on Twitter is outlined in the company's terms of service agreement, 'The Twitter Rules', which were significantly updated in

[46] Courtney Boyd Myres, '5 years ago today Twitter launched to the public' (*TNW*, 15 July 2015) <https://thenextweb.com/twitter/2011/07/15/5-years-ago-today-twitter-launched-to-the-public/> accessed 28 February 2019
[47] Ursula Smartt, *Media & Entertainment Law* (Taylor & Francis 2017) 79
[48] Alex Hern, 'Twitter further tightens abuse rules in attempt to prove it cares' *The Guardian* (London, 18 October 2017) <https://www.theguardian.com/technology/2017/oct/18/twitter-abuse-rules-jack-dorsey-hate-speech-revenge-porn-violent-groups-social-network> accessed 17 January 2019
[49] Twitter, 'Our approach to policy development and enforcement philosophy' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/enforcement-philosophy> accessed 3 January 2019

2017.[50] The Twitter Rules have been created through in-depth research examining online discourse, with the company being aided by around forty not-for-profit organisations.[51] Here, Twitter's Rules are considered to be guided by transparency and empowerment, where freedom of speech will prevail.[52] The discussion below will outline Twitter's terms of service agreements governing hate speech, abusive behaviour, credible threats of violence and revenge pornography.

Twitter and Hate Speech

Twitter defines hate speech as violence, direct attack or threatening behaviour against another:

> '… on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease.'[53]

The Twitter Rules therefore prohibit content which is motivated by hate, prejudice or intolerance, which targets one of the above protected characteristics.[54] For Twitter, hateful content can take many forms for instance, targeting others with reference to mass murder or violent events, inciting fear about a sector of society, including promoting exclusion of others from a given situation, and unsolicited hateful imagery.[55] Though these comments alone may not be in breach of Twitter's guidelines, instead, it

---

[50] Hern n.48
[51] *Ibid.,*
[52] Twitter, 'Legal request FAQs' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/twitter-legal-faqs> accessed 3 January 2019
[53] Twitter, 'Hateful conduct policy' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy> accessed 3 January 2019
[54] *Ibid.,*
[55] Twitter, 'Twitter Rules Enforcement' (*Twitter*, 2018) <https://transparency.twitter.com/en/twitter-rules-enforcement.html#twitter-rules-enforcement-jan-jun-2018> accessed 18 February 2019

needs to be clear that the person being targeted falls within one of the protected characteristics above. Between January and June 2018 Twitter took action[56] against 285,393 accounts for breaching its hate speech guidelines.[57]

Despite a clear definition given by Twitter as to what constitutes hate speech, on several occasions representatives from Twitter have been brought before Parliamentary Committees to discuss the continued issue of hate speech on its site. For instance, in 2017 the Home Affairs Committee raised concerns about images on Twitter which they considered to be racist, an example of which is shown in figure five. In addition, one image which contained the hashtag 'Deport all Muslims', was flagged by the committee as inciting hate; yet Twitter concluded that the image in question did not breach its terms.[58] Consequently, the image was allowed to remain on Twitter.

Figure 5: *Tweets intended to stir up hatred against ethnic minorities which the Home Affairs Committee reported to Twitter*. [59]

[56] Twitter uses '… the term "action" to refer to our range of enforcement actions, which include possible account suspension', *Ibid.,*
[57] Twitter n.55
[58] Home Affairs Committee, *Oral Evidence: Hate Crime and its Violent Consequences* (HC 2017, 609) Q37-39
[59] Home Affairs Committee n.7, [13]

Similarly, the Fawcett Society in August 2017 openly criticised Twitter in a public letter, following their slow removal of content reported by the Fawcett Society:

> 'Numerous examples of abuse, threats, and hate speech on the platform were identified and reported early last week [week commencing 14 August] - by the morning of the 21st August they were still up on the platform, despite the fact that they clearly violate Twitter's own community standards that do not allow direct or indirect threats or can be categorised as harassment or hateful content. No response has been sent to the people who reported them, and no action had been taken against the users who posted them.'[60]

The week before the public letter was sent to Twitter, members of the Fawcett society reported content which they believed to be in clear breach of Twitter's guidelines. This included the organisation of a protest by white supremacists and anti-Semitic abuse aimed a Liverpudlian MP Luciana Berger.[61] A week later the content remained on the site yet within hours of the Fawcett society's letter going public, the tweets were removed.

Like that of Facebook hate speech is evidently present on Twitter, with the company accepting that mistakes have been made.[62] Nonetheless, Twitter continues to be slow in the removal of hate content from its site.[63]

---

[60] The Fawcett Society, 'Twitter is "failing women" experiencing online threats and harassment' (*The Fawcett Society*, 22 August 2017) <https://www.fawcettsociety.org.uk/news/twitter-failing-women-experiencing-online-threats-harassment> accessed 16 February 2018

[61] *Ibid.,*

[62] Hern n.48

[63] Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018) [2.151]

Twitter and Bullying

Unlike Facebook Twitter does not have terms of services dealing specifically with bullying, instead, all unwelcomed conduct falls within 'abusive behavior' [*sic*]. Between January and June 2018, 248,629 accounts were action by Twitter for abusive behaviour.[64] Twitter defines abusive behaviour as conduct that harasses, intimidates or reduces another person's speech,[65] though emphasis is placed on ensuring freedom of speech is maintained on the site: '[w]e [Twitter] believe that everyone should have the power to create and share ideas and information instantly, without barriers.'[66]

For Twitter, context is a key consideration in determining if certain content should be removed from the site:

> 'Some [t]weets may seem to be abusive when viewed in isolation, but may not be when viewed in the context of a larger conversation. When we [Twitter] review this type of content, it may not be clear whether it is intended to harass an individual, or if it is part of a consensual conversation.'[67]

To determine the context of a tweet several factors are taken into account by Twitter. First, who is the intended target of the abuse; second, is there a public interest element justifying the tweet to remain on the site; third, who reported the complained about behaviour.[68]

Any Twitter user can report content which they believe to be in breach of the Twitter Rules. Once reported, moderators, discussed further in later parts of

---

[64] Twitter n.55
[65] Twitter, 'Abusive behavior' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/abusive-behavior> accessed 3 January 2019
[66] *Ibid.,*
[67] *Ibid.,*
[68] *Ibid.,*

this chapter, will determine if the content breaches Twitter's guidelines. There are no limits on who can report abusive behaviour, though Twitter maintains that abusive content, which is not directly reported from the victim, may not necessarily be removed from its site:

> 'To help our teams understand the context of a conversation, we [Twitter] may need to hear directly from the person being targeted, to ensure that we have the information needed prior to taking any enforcement action.'[69]

The onus is therefore placed on the victim to report comments which can be considered abusive, which can be extremely difficult in dogpiling situations.

As detailed in chapter one dogpiling is the situation whereby a user or users actively encourages another to 'attack' others online. This can result in a person receiving multiple abusive messages. For instance, Jess Phillips MP, as will be discussed at varies points in this thesis, has spoken about receiving more than 600 threats of rape in one night alone *via* Twitter.[70] Similarly, Caroline Criado-Perez an active feminist campaigner received 50 abusive tweets per hour following her campaign to get Jane Austin printed on banknotes in England and Wales.[71] In these situations, it can be impossible for all comments to be reported, especially by the person being attacked.

---

[69] *Ibid.,*
[70] Sally Hayden, 'Labour's Jess Phillips received "600 rape and death threats in a single day"' *The Independent* (London, 27 August 2017) <http://www.independent.co.uk/news/uk/home-news/labour-mp-jess-phillips-rape-death-threats-one-day-social-media-attacks-training-a7915406.html> accessed 25 October 2017
[71] The BBC, 'Caroline Criado-Perez Twitter abuse case leads to arrest' *The BBC* (London, 29 July 2013) <https://www.bbc.co.uk/news/uk-23485610> accessed 8 February 2019

Twitter and Credible Threats

Twitter prohibits '…specific threats of violence or [the] wish for the serious physical harm, death, or disease of an individual or group of people.'[72] The abuse experienced by Jess Phillips and Caroline Criado-Perez, as discussed above, are clear examples of credible threats of violence. For instance, both women received explicit tweets threatening sexual assault and physical injury:

> '… someone was talking about giving me a good smashing up the arse. Somebody said: "All aboard the rape train." Some guy tweeted another guy asking if he wanted to join in raping me. Then there were the death threats. One was from a really bright guy who said: … "I'd do a lot worse than rape you. I've just got out of prison and would happily do more time to see you berried [*sic*]".'[73]

Many of these comments aimed at Jess Phillips and Caroline Criado-Perez, were not removed by Twitter, despite a clear breach of their terms of service agreement.[74]

Credible threats of violence remain problematic for Twitter users.

Recent research has uncovered many examples of threatening behaviour on Twitter. For instance, research undertaken by Amnesty International

[72] Twitter, 'Violent threats and glorification of violence' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/violent-threats-glorification> accessed 3 January 2019

[73] Caroline Criado-Perez, see, Simon Hattenstone, 'Caroline Criado-Perez: '"Twitter has enabled people to behave in a way they wouldn't face to face"' *The Guardian* (London, 4 August 2013) <https://www.theguardian.com/lifeandstyle/2013/aug/04/caroline-criado-perez-twitter-rape-threats> accessed 8 February 2019

[74] Kevin Rawlinson, 'Twitter faces boycott after "inaction" over rape threats against feminist bank notes campaigner Caroline Criado-Perez' *The Independent* (London, 27 July 2013) <https://www.independent.co.uk/news/uk/home-news/twitter-faces-boycott-after-inaction-over-rape-threats-against-feminist-bank-notes-campaigner-8734856.html> accessed 8 February 2019. Between January and June 2018, 47,9251 accounts were actioned for breaching Twitter's credible threats policy. See, Twitter n.55

uncovered numerous tweets threating both sexual and physical violence against women on the site: [75]

> 'Online abuse began for me when I started the Everyday Sexism Project – before it had become particularly high-profile or received many entries. Even at that stage, it was attracting around 200 abusive messages a day. The messages included detailed, graphic, and explicit descriptions of rape and domestic violence.'[76]

Despite this, Twitter maintains that threats are not permitted on its site: '[a]buse and hateful conduct directed at women, including direct threats of violence, and harassment, are prohibited on Twitter.'[77] However, to be in breach of Twitter's guidelines the threat needs to be direct, credible and specific.[78] So, for instance a comment stating 'I will kill you' may not be in breach of Twitter's Rules.

In recent years, Twitter has been used to directly threaten another, particularly women, online:

> 'As a company, Twitter is failing in its responsibility to respect women's rights online by inadequately investigating and responding to reports of violence and abuse in a transparent manner.'[79]

Amnesty International over a 16 month period conducted qualitative and quantitative research, to illustrate the continued use of sexual threats against women on Twitter.[80] Using interviews, focus groups and questionnaires they

---

[75] Amnesty International, 'Toxic Twitter- A Toxic Place For Women' (*Amnesty International*, 2017) <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/> accessed 18 January 2019
[76] Laura Bates, 'Laura Bates: Violence Against Women Online' (*Amnesty International*, 21 March 2018) <https://www.amnesty.org/en/latest/research/2018/03/laura-bates-online-violence-against-women/> accessed 23 January 2019
[77] Amnesty International n.75
[78] Twitter n.72
[79] Amnesty International n.75
[80] Amnesty International, 'Toxic Twitter- Methodology' (*Amnesty International*, 2017) <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-methodology/> accessed 18 January 2019

were able to expose how women are being subjected to explicit threats of sexual violence in order to reduce their voices online, despite this being a clear breach of Twitter's guidelines.

Twitter has specific guidelines prohibiting credible threats of violence. However, these guidelines are not always being adequately applied to conduct that is in clear breach of the Twitter Rules. The lack of consistency in Twitter's guidelines is further illustrated in the company's approach to the removal of revenge pornography, as discussed below.

Twitter and Revenge Pornography

As outlined in chapter one and discussed further in chapter five, revenge pornography is becoming a significant problem within society. In recent years Twitter has attempted to strengthen its terms of service agreements to help tackle revenge porn on its site.[81] Like that of Facebook, revenge pornography is prohibited on Twitter:

> 'You may not post or share intimate photos or videos of someone that were produced or distributed without their consent. Media depicting sexual violence and/or assault is also not permitted.'[82]

Unlike Facebook Twitter lacks specific criterions for the removal of content which can be labelled as revenge porn, demonstrated in a high-profile example of revenge pornography in July 2017.

[81] Hern n.48
[82] Twitter, 'About intimate media on Twitter' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/intimate-media> accessed 18 January 2019

Rob Kardashian a reality star from the hit American TV show 'Keeping up with the Kardashian's', took to Twitter to post explicit images of his ex-girlfriend, Blac Chyna, after an argument.[83] The tweet contained abusive commentary alongside images of her genitalia and a sex tape. These images were actively shared across the social media site by some of his 7 million followers, with the behaviour of Kardashian being reported worldwide. Despite this clear breach of Twitter's guidelines, Kardashian was not suspended from the site instead, the original post was removed by Twitter.[84]

Similarly, research undertaken by the Fawcett Society as discussed above, uncovered revenge porn videos which were reported to the company, but subsequently ignored. One of the videos found by the Fawcett Society contained graphic images of an apparent rape. Despite reporting this video to Twitter, the content remained on Twitter for a further week.[85] Twitter, like that of many other social media sites, is struggling to keep pace with the extent of revenge pornography on its site, despite community guidelines in place prohibiting the behaviour.

Summary

Like that of Facebook, Twitter accepts that it has made mistakes in its application of its Twitter Rules to content that is posted on its site.[86] It has at

[83] Alex Heath, 'Twitter outlines how it will be tougher on banning revenge porn' *Business Insider UK* (London, 27 October 2017) <https://www.businessinsider.com/twitter-tougher-revenge-porn-backlash-2017-10?r=UK> accessed 18 January 2018
[84] Note, Kardashian also uploaded the same pictures to Instagram, another social media site run by Facebook, who suspended the account. *Ibid.,*
[85] The Fawcett Society n.60
[86] Heath n.83

times allowed extremely abusive and illegal behaviour to remain publicly viewable, and there is a clear lack of consistency in the application of its terms of service agreement against user-generated content. The following discussion will outline how both Facebook and Twitter are attempting to tackle the growing issue of online abuse on their sites.

Tackling Unlawful Behaviour

Despite terms of service agreements between users and social media companies, it is clear from the discussion above that issues continue to arise with bullying, threats, hate speech and revenge pornography. Both Facebook and Twitter are continuing to tackle these issues through a variety of different mechanisms. The following sections will outline some of the mechanisms used by Facebook and Twitter in order to tackle the growing problem of inappropriate behaviour on their sites. This will include examining the use of moderators on Facebook and Twitter, the implementation of Artificial Intelligence (AI) Technology, Facebook's bullying prevention hub, and Twitter's use of content blockers, before turning to look at how both companies aid law enforcement.

Moderation

A common mechanism used by both Facebook and Twitter in reducing inappropriate content on their sites is the use of moderators. Here, individuals are employed to review content, which in many cases has been flagged by other online users, to determine if the content should remain on the site. To do this, moderators apply the complained about behaviour to the

terms of service agreements to establish if the user has breached the company's guidelines. As discussed in the previous chapter, for Williams to reduce criminality suitable guardians need to be in place.[87] Yet, a whistle-blower at Facebook has claimed that the high number of posts means that in many cases moderators have less than ten seconds to make a decision, meaning mistakes are often made,[88] with offensive behaviour on the increase.

In the past, Facebook has been reluctant to disclose information regarding its moderation team.[89] Despite this, before the US Congress Mark Zuckerberg spoke in detail about self-regulation and the use of moderators to determine what content should, or should not, remain on the site. For Zuckerberg, currently the only way to tackle hate speech on its site is through the use of moderators, and therefore Facebook has invested more money into expanding its moderation team.[90] By the end of 2018 he anticipated that the company would have around 20,000 moderators, working across 7 states, twenty-four hours a day to review content flagged by users.

Facebook moderators have several options available when reviewing posts, which are determined based on the company's community guidelines. For instance, if the moderator concludes that the flagged content does not breach Facebook's community standards, then the post will be allowed to

[87] Katherine S. Williams, *Textbook on Criminology* (7th edn, Oxford University Press 2012) 312
[88] Hopkins n.41
[89] Home Affairs Committee, n.58, Q571
[90] Guardian News n.10

remain on the site even if it is objectionable to some. For example, as discussed previously the comment, 'to snap a bitch's neck, make sure you apply all the pressure to the middle of the throat', was allowed to remain on Facebook, as it was concluded that the comment did not breach the company's community standards.[91] Whereas comments which are found to be in breach of Facebook's terms of service agreement, can be removed or the person who posted the content can be suspended from the site.[92]

Likewise, Twitter employs moderators to review content which has been reported by its users. Yet it is currently unknown how many moderators are employed by Twitter though it is thought to be in the thousands.[93] Like that of Facebook, Twitter moderators review any content that is flagged by users as breaching the terms of the site, though the outcomes do differ between the two companies. Whereas in most cases Facebook will either allow a post to remain on its site, remove the post or suspend the user, Twitter moderators are given more options. Here, if the flagged content is considered as breaching the Twitter Rules, moderators can choose to make a person's Twitter page 'read-only'. Read-only accounts allow the Twitter users profile to remain viewable to the public, but no content can be posted on the site until the user has removed the prohibited tweet.[94] An overriding reason why

[91] Nick Hopkins, 'Facebook moderators: a quick guide to their job and its challenges' *The Guardian* (London, 21 May 2017) <https://www.theguardian.com/news/2017/may/21/facebook-moderators-quick-guide-job-challenges> accessed 21 January 2019
[92] *Ibid.,*
[93] Home Affairs Committee n.58, Q571
[94] Twitter, 'Our range of enforcement options' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/enforcement-options> accessed 21 January 2019

Twitter allows this option to be available is to ensure freedom of speech is not curtailed.[95]

However as discussed above, Twitter has been criticised for being slow in the removal of content which is in clear breach of their guidelines.[96] As will be outlined in chapter eight, in 2016 the European Commission introduced a Code of Conduct aimed at social media companies to create guidelines in tackling inappropriate content.[97] Twitter has agreed with the European Commission to remove unlawful content from its site within 24 hours.[98] Yet examples will be given throughout this thesis of Twitter failing to remove unlawful tweets within the 24 hour time limit set out by the European Commission.[99]

Despite the need for moderators on sites like Facebook and Twitter, the number of comments generated on the sites means that moderators are often overwhelmed by content which needs to be reviewed.[100] In addition, there continues to be issues with language and the time taken to remove content which violates social media terms of services.[101] Consequently, both

[95] Twitter n.65
[96] For example, The Fawcett Society n.60
[97] Commission, 'Tackling Illegal Content Online: Towards an enhanced responsibility of online platforms' COM (2017) 55 final 2. Note, this is not legally binding on social media sites.
[98] *Ibid.,*
[99] For example, see, Gordon Rayner & Kate McCann, 'Twitter is "failing women" by taking too long to remove misogynistic abuse, Yvette Cooper says' *The Telegraph* (London, 22 August 2017) <https://www.telegraph.co.uk/news/2017/08/21/twitter-failing-women-taking-long-remove-misogynistic-abuse/> accessed 9 February 2019
[100] Hopkins n.91
[101] Guardian News n.10

Facebook and Twitter are investing in AI technology to help tackle the growing issue of unlawful behaviour online.

AI Technology

AI technology:

> '… is an area of computer science that emphasizes [*sic*] the creation of intelligent machines that work and react like humans. Some of the activities computers with artificial intelligence are designed for include: [s]peech recognition, [l]earning, [p]lanning and [p]roblem solving.'[102]

AI technology has been implemented into the computer systems of both Facebook and Twitter, to review content before it becomes publicly viewable.[103] In fact, over 99% of terrorist propaganda removed by Facebook is flagged by AI technology:[104]

> '… one of our [Facebook] greatest opportunities to keep people safe is building artificial intelligence to understand more quickly and accurately what is happening across our community.'[105]

During Facebook's hearings before both Congress and the European Parliament, Mark Zuckerberg emphasised the need to invest in AI technology to help moderate online content, allowing Facebook to become more proactive rather than reactive to unlawful content on its site.[106] This is particularly true regarding revenge pornography, where Facebook has created AI technology to recognise sexually explicit pictures. Nonetheless, for AI technology to be successful in reducing revenge pornography,

---

[102] Techopedia, 'Artificial Intelligence (AI)' (*Techopedia*, 2019) <https://www.techopedia.com/definition/190/artificial-intelligence-ai> accessed 21 January 2019
[103] Home Affairs Committee n.58, Q679
[104] Guardian News n.10
[105] Mark Zuckerberg n.20
[106] PBS NewsHour n.11

Facebook has indicated the need for users to allow the company access to their sexually explicit images:

> 'It's demeaning and devastating when someone's intimate images are shared without their permission, and we [Facebook] want to do everything we can to help victims of this abuse. We're [Facebook] now partnering with safety organizations [*sic*] on a way for people to securely submit photos they fear will be shared without their consent …'.[107]

In England and Wales this would mean users would be able to contact the Revenge Porn Helpline to obtain a link to upload their intimate images. These pictures would then be 'scrambled' by technology at Facebook and remain on its servers. If someone later attempted to upload the image to Facebook, the AI technology will flag the image and the image would not be posted.[108]

Similarly, Twitter has also empathised the importance of AI technology to ensure its terms of service agreement is not being breached.[109] Yet Twitter has been reluctant to share publicly the advancements of its technology to help combat online abuse.[110] Despite the advancements in AI technology in recent years, there currently remains problems with the use of AI technology in tackling hate speech and abusive commentary on social media sites.[111]

As illustrated above and throughout this thesis, there remains a prominent issue of hate speech and abusive commentary on Facebook and Twitter. AI

[107] The BBC, 'Facebook wants your naked photos to stop revenge porn' *The BBC* (London, 23 May 2018) <https://www.bbc.co.uk/news/newsbeat-44223809> accessed 23 January 2019
[108] *Ibid.,*
[109] Home Affairs Committee n.58, Q679
[110] *Ibid.,*
[111] *Ibid.,*

technology is currently unsuccessful when it comes to hate speech and online abuse. As explored in detail in chapter one, Facebook in 2018 made available to the public for the first time, a transparency report exposing the scale of abuse on its site. In one six-month period 4.1 million posts were removed from Facebook for breaching its hate speech community standards.[112] The report also contained information regarding how Facebook was made aware of the posts. In the majority of situations, the unlawful content came to the attention of Facebook moderators by other Facebook users, as opposed to AI Technology with Alex Schultz, the company's head of data analytics, commenting:

> '… there's context that technology just can't do yet … So, in those cases [hate speech and abusive commentary] we [Facebook] lean a lot still on our review team, who makes a final decision on what needs to come down.'[113]

This was reflected further by Mark Zuckerberg, who suggested that it would be another 5 to 10 years before AI technology would be fully successful in the removal of hate speech and abusive commentary from its site.[114] In the meantime, other forms of governance need to be strengthened, such as Facebook's bullying prevention hub.

Bullying Prevention Hub: Facebook

In an attempt to support victims of cyberbullying, in 2013 Facebook launched its bullying prevention hub,[115] being one of the first social media companies

---

[112] Dave Lee, 'Facebook details scale of abuse on its site' *The BBC* (London, 15 May 2018) <http://www.bbc.co.uk/news/technology-44122967> accessed 29 May 2018
[113] *Ibid.,*
[114] PBS NewsHour n.11
[115] Facebook, 'Bullying Prevention Hub' (*Facebook*, 2019) <https://www.facebook.com/safety/bullying> accessed 3 January 2019

to '… integrate bullying prevention tools directly into a product.'[116] The aim of the bullying prevention hub is to arm:

> '… bullying victims with information on what they can do when they see harassing content, recommendations to adults who want to help, and even guidance to the person accused of bullying on what he or she has done and how he or she can do better.'[117]

The bullying prevention hub which is available through Facebook's community standards is aimed at minors, parents and educators. The hub contains step-by-step instructions to support victims of cyberbullying.[118]

Individuals can download help sheets which have been created with the aid of Yale Centre for Emotional Intelligence. These help sheets include proactive advice to those who have become subjected to cyberbullying. So, for instance the victim is advised to tell an adult they trust, whilst also detailing tools located on Facebook to aid the person being bullied. For example, how to unfriend[119] or block[120] the perpetrator of the abuse.[121]

Though the bullying prevention hub is not directly tackling cyberbullying, it does give victims proactive options to help them in a time of emotional distress. Emphasis is placed on educating Facebook users, which in turn

---

[116] Facebook, 'Facebook Safety' (*Facebook*, 6 November 2013) <https://www.facebook.com/fbsafety/posts/today-we-are-launching-the-new-bullying-prevention-hub-offering-important-tools-/600514153319760/> accessed 9 February 2019
[117] *Ibid.,*
[118] Facebook n.115
[119] Unfriending a person means that they cannot see private content on a person's Facebook page. However, all content that is public is still viewable, along with the person who has been unfriended being able to contact the user. See, Facebook, 'Bullying Prevention Hub: Teens' (*Facebook*, 2019) <https://www.facebook.com/safety/bullying/teens> accessed 3 January 2019
[120] Blocking a person means that they are unable to see any aspect of the blockers Facebook page. *Ibid.,*
[121] *Ibid.,*

empowers the person being targeted '[r]ather than simply focus on awareness of this information, we're [Facebook] putting it at people's fingertips at the moment they need it most [*sic*].' Yet cyberbullying continues to be an issue for Facebook. As discussed in chapter one Ditch the Label conducts an annual bullying survey in the United Kingdom. In their 2018 findings, 66%[122] of participants experienced some form of cyberbullying, of which 37% had experienced cyberbullying on Facebook.[123] Despite the clear need for the bullying prevention hub on Facebook, it is not directly tackling the growing issue of cyberbullying.

Content Blocking: Twitter

Whereas Facebook is educating its users, Twitter is using the advancement of technology to reduce what its users see on their profiles. In 2017 Twitter updated its platform to allow users to have more control with regard to content on its site:

> 'You might see content in [t]weets you'd like to avoid. We [Twitter] give you the option to mute [t]weets that contain particular words, phrases, usernames, emojis, or hashtags.'[124]

With the aid of technology, an online user can now block certain content from their Twitter feed. For example, in the past a victim of dogpiling would have had to either tolerate the abuse they were receiving, whilst waiting for Twitter to decide on any comments which had been reported, or closedown their

[122] Over 9000 individuals took part in the survey.
[123] Ditch the Label, 'The Annual Bullying Survey 2017' (*Ditch the Label*, 2017) 26 <https://www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-1.pdf> accessed 9 February 2018
[124] Twitter, 'How to use advanced muting options' (*Twitter*, 2019) <https://help.twitter.com/en/using-twitter/advanced-twitter-mute-options> accessed 3 January 2019

Twitter account. Now, if there is a particular word or hashtag associated with the abuse, the user can mute that specific word or hashtag to reduce their likelihood of seeing the abuse.[125] For instance, Caroline Criado-Perez,[126] as mentioned above, could have muted words, such as 'fuck', 'rape' and 'witch' to reduce the likelihood of seeing the abusive messages. Nevertheless, this technological advancement by Twitter does not directly stop abuse from occurring, it simply hides it from the person being abused.

The content muting option contained on Twitter can be considered as a step forward in helping those who are targeted on its site. However, like that of Facebook's bullying prevention hub, it allows for abusive commentary to remain on its site, so long as it does not breach the Twitter Rules. It also places an onus on victims to highlight key phrases associated with their abuse, a factor which may be considered as distressing for some. As detailed in chapter seven online abuse can have a significant effect on a person's physiological integrity, which in some cases has resulted in suicide. The process of highlighting key phrases associated with a person's abuse would add further pressure on a person who may already be significantly fragile due to the abuse they are receiving.

Law Enforcement

Both Twitter and Facebook maintain within their terms of service agreements that they will work with law enforcement when there are serious breaches of

[125] *Ibid.,*
[126] For an in-depth discussion of the abuse experienced by Caroline Criado-Perez, see chapter four.

the law.[127] Though, both companies maintain that certain criterions need to be established first before they will provide law enforcement with private individual data.

For Twitter, information will only be shared with law enforcement where there is a valid legal process governed by applicable law.[128] Here, the legal request would have to be submitted to the appropriate Twitter Headquarters.[129] So, for example requests by the police in England and Wales have to be made to Twitter's office based in Dublin, in which the request needs to be specific: 'Twitter may file or serve objections for requests that are legally defective, overly broad, and/or appear to impermissibly burden free expression.'[130] Between January and June 2018, Twitter narrowed or refused to give the information requested by law enforcements, across 53 countries worldwide, in 46% of cases.[131] During this period law enforcement in the United Kingdom submitted 947 account information requests, with 30% of these requests being unsuccessful.[132]

[127] Facebook, 'Information for law enforcement authorities' (*Facebook*, 2019) <https://www.facebook.com/safety/groups/law/guidelines/> accessed 3 January 2019. Twitter, 'Guidelines for law enforcement' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support> accessed 3 January 2019
[128] Twitter, 'Guidelines for law enforcement' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support> accessed 3 January 2019. Note, there are different rules for emergency requests.
[129] *Ibid.,*
[130] Twitter, 'Legal request FAQs' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/twitter-legal-faqs> accessed 3 January 2019
[131] Twitter, 'Transparency Report: Information Requests' (*Twitter*, 2018) <https://transparency.twitter.com/en/information-requests.html> accessed 24 January 2019. This figure does not include emergency requests.
[132] *Ibid.,*

Similarly, Facebook maintains that it will disclose information to law enforcement both inside and outside the United States where the request is in accordance with their terms of service agreement, and applicable legal provisions.[133] Like that of Twitter, Facebook has produced a transparency report exposing the number of law enforcement requests they have received in recent years. Between January and June 2018 Facebook received 103,815 requests from government organisations requesting user information, across 102 countries worldwide.[134] In total Facebook did not disclose any information in 26% of cases.[135] The United Kingdom during the same period made 6,538 requests for user information, in which Facebook complied with the request in 91% of cases.[136]

In a time where nearly half of all crimes reported to the police in England and Wales, involves some form of social media, social media companies need to work alongside law enforcement.[137] The discussion above has exposed the continuing issues with content posted on social media sites, from hate speech to revenge pornography. Though Twitter and Facebook maintain in their terms of service agreements that they will work alongside governments and the police when it comes to unlawful conduct, they have been slow in aiding law enforcement. The slow approach of social media sites in helping

[133] Facebook n.127
[134] Facebook, 'Government Requests for User Data' (*Facebook*, 2018) <https://transparency.facebook.com/government-data-requests/jan-jun-2018> accessed 24 January 2019
[135] *Ibid.,* note, figure includes emergency requests.
[136] *Ibid.,*
[137] Kate McCann, 'Social media giants should be forced to pay for policing social media, report backed by Amber Rudd claims' *The Telegraph* (London, 1 May 2017) <https://www.telegraph.co.uk/news/2017/04/30/social-media-giants-should-forced-pay-policing-social-media/> accessed 24 January 2019

the police was highlighted in September 2018 following the murder of a schoolgirl in the United Kingdom.[138]

Lucy McHugh was raped and murdered in July 2018. Following her death, Stephen-Alan Nicholson was arrested and subsequently found guilty of her murder. During the early stages of his arrest Southampton Police, approached Facebook to gain access to Nicholson's social media page, where the company initially failed to provide vital information about Nicholson to the police.[139] Detectives involved in the case accused Facebook of taking an 'inordinate amount of time' before allowing them access to his account, putting emotional distress upon Ms McHugh's family.[140] Consequently, despite specific guidelines being in place, Facebook and Twitter are failing to adequately help law enforcement.

Chapter Overview

The discussion above illustrates just some of the ways in which Facebook and Twitter are attempting to limit inappropriate behaviour on their sites. None of the approaches are perfect, with mistakes being made. One of the major issues surrounds the inconsistency of terms of service agreements and its application to 'real-life' scenarios. Facebook has shutdown activism,

---

[138] Alex Hern, 'Why won't Facebook give access to Lucy McHugh murder suspect's account?' *The Guardian* (London, 5 September 2018) <https://www.theguardian.com/uk-news/2018/sep/05/why-wont-facebook-provide-access-lucy-mchugh-suspect-account> accessed 24 January 2019. See also, Fiona Hamilton, 'Police wait 18 months for evidence from social media firms' *The Times* (London, 14 September 2018) <https://www.thetimes.co.uk/article/police-wait-18-months-for-evidence-from-social-media-firms-6djhnwcj0> accessed 24 January 2019

[139] The BBC, 'Lucy McHugh death: "Challenge" over accessing Facebook information' *The BBC* (London, 4 September 2018) <https://www.bbc.co.uk/news/uk-england-hampshire-45408338> accessed 9 February 2019

[140] *Ibid.,*

whilst hate speech has been allowed to remain on its site. In addition, Twitter has allowed threats to remain on its server, despite numerous requests for its removal. Clearly more needs to be done by social media companies to help tackle abusive behaviour online, highlighted further in chapter nine. The following chapter will discuss how the law is currently being applied in a social media setting, through the lens of legality.

Chapter Three: Recommendations

- Create a universal code of conduct aimed at all social media companies to ensure they are protecting individuals from online abuse. This universal code of conduct will be created in a clear and precise manner;
- Ensure social media companies are transparent with their users;
- Updated and regular training for moderators;
- Any legal provisions that are created ensures that the advancement of new technology or new social media companies are not restricted;
- Ensure social media companies aid law enforcement; and
- Where social media companies fail to comply with the universal code of conduct create a punishment process in the form of a fine, governed by the e-Safety Commissioner.

Chapter Four

Social Media, Criminal Law Regulation and Non-Technology-Based Legislation

> 'Governments in the United Kingdom, Canada and the United States and other countries of the world struggle to draft legislation in order to deal with this growing threat to the new electronic global community commonly called the Internet.'[1]

In England and Wales there is no specific Act of Parliament that governs conduct carried out online, especially in relation to social media. Instead, the criminal law has been shaped and adapted to cover an online context. The current criminal law framework in England and Wales used to prosecute social media abuse can be split into two categories: technology-based, and non-technology-based legislation. Essentially, there are some Acts that have been created by Parliament to legislate against technology-based offences, though these were not necessarily created with social media in mind.[2] These legal provisions will be discussed in detail in chapters five and six.

In the following discussion non-technology-based legislation which has been used to criminalise social media conduct will be critically evaluated, this will include: the Serious Crime Act 2007, the Public Order Act 1986 and the Protection from Harassment Act 1997. Each law will be taken in turn, explained and critically examined in relation to it's use in a social media context.

---

[1] Ahmad Nehaluddin, 'Hackers' criminal behaviour and laws related to hacking' (2009) 15(7) Computer and Telecommunications Law Review 159, 160

[2] For instance, the Malicious Communications Act was enacted in 1988 with the first social media site 'Six Degrees' not being publicly available until 1997. See, Laura Scaife, *Handbook of Social Media and the Law* (Routledge 2015) 4

Serious Crime Act 2007

The Serious Crime Act 2007 made a number of radical changes to the criminal law during its implementation.[3] The Act originally made no mention of technology, the Internet or social media until it was updated in 2015.[4] Despite this, it was used to prosecute several individuals for social media related offences following the 2011 riots in the UK.[5] Its use to prosecute these cases invoked criticism from MPs and the media, with arguments suggesting that the defendant's sentences were 'too severe'.[6] In this discussion part two sections 44 to 46 of the Serious Crime Act will be critically examined, looking in detail at both the *actus reus* and *mens rea* of the offences criminalised under these sections. Before this, the background surrounding the enactment of the Serious Crime Act will be outlined, demonstrating how its use in a social media context falls outside the mischief of the Act. It will be put forward in the following discussion that the use of the Serious Crime Act to govern social media is uncertain, breaching the fundamental principles of legality.

After several consultation papers conducted on behalf of the Government the Serious Crime Act 2007 received Royal Assent on 30 October 2007, aiming:

> '… to make provision[s] about serious crime prevention orders; to create offences in respect of the encouragement or assistance of crime; to enable information to be shared or processed to prevent

[3] For the purpose of this discussion only Part Two of the Serious Crime Act 2007 will be considered, as this is the only part of the Act which is relevant in a social media context.
[4] The Serious Crime Act 2007 Schedule One was implemented into the Act by The Serious Crime Act 2015 section 47(4)
[5] *R v Blackshaw* [2011] EWCA Crim 2312, [2012] 1 W.L.R. 1126
[6] Andy McSmith, 'Tough riot sentences prompt new guidelines for the courts' *The Independent* (London, 17 August 2011) <http://www.independent.co.uk/news/uk/crime/tough-riot-sentences-prompt-new-guidelines-for-the-courts-2339699.html> accessed 20 January 2018

fraud or for purposes relating to proceeds of crime ...'.[7]

The purpose of the Act was to tackle the ever-growing issue of organised crime within society, which was estimated to be worth £20 billion per year.[8]

Organised crime is '… serious crime planned, coordinated and conducted by people working together on a continuing basis. Their motivation is often, but not always, financial gain.'[9] In 2013 a consultation paper examining serious and organised crime suggested that this behaviour was a threat to national security, and the law needed to be updated to reflect the 'seriousness' of the offence.[10] In 2015 the Serious Crime Act was amended by the Serious Crime Act 2015 to reflect the growing need to protect the state from terrorism.[11]

In the 2007 Act a list of offences can be found which are defined as 'serious crime', with many of these being added into the Act following the 2013 consultation.[12] These offences include drug trafficking, slavery, people trafficking, firearm offences, prostitution and child sex, armed robbery, money laundering, fraud, offences in relation to public revenue, bribery, counterfeiting, computer misuse, intellectual property, the environment and organised crime and inchoate offences.[13] Though the Serious Crime Act

---

[7] Serious Crime Act 2007
[8] Home Office, *One Step Ahead: A 21st Century Strategy to Defeat Organised Crime* (CM 6167, 2004) 8
[9] National Crime Agency, 'Organised Crime Groups' *(NCA*, 2017) <http://www.nationalcrimeagency.gov.uk/crime-threats/organised-crime-groups> accessed 2 January 2018
[10] HM Government, *Serious and Organised Crime Strategy* (CM 8715, 2013) [1.3]
[11] *Ibid.,*
[12] The Serious Crime Act 2015. See also, David S Wall & Yulia Chistyakova, 'How organised crime in the UK has evolved beyond the mafia model' *The Conversation* (London, 18 May 2015) <https://theconversation.com/how-organised-crime-in-the-uk-has-evolved-beyond-the-mafia-model-40782> accessed 2 January 2018
[13] Serious Crime Act 2007 Schedule One

arguably now covers technology-based crime, this is from an organised criminal perspective, commonly referred to as cybercrime:

> 'Cyber-enabled crime allows crime on a significant scale: a single "phishing" email (an email where the sender purports to be a trustworthy entity to secure financial or other details) can be used to target very large numbers of people ...'.[14]

Thus, from an examination of the Serious Crime Act the Act is still not intended to cover social media abuse between two or more private individuals.

The emphasis under the Serious Crime Act is placed on targeting those who pose the most substantial threats to the public. The 'seriousness' element was highlighted throughout the consultation period prior to the Act receiving Royal Assent:

> 'The Law Commission's proposals form an excellent starting point for looking at the best way to achieve this [deal with organised crime efficiently], and offences suggested above build on this in relation to organised crime. They will target those on the periphery of organised crime who are difficult to prosecute under the existing legal framework.'[15]

Several key provisions are found under the Act, many of these aimed at tackling the mischief behind the Serious Crime Act, combatting organised crime. For instance, the Act created Serious Crime Prevention Orders. These orders are like Anti-social behaviour orders commonly referred to as ASBOs but have more extensive powers. For instance, it can be used to restrict where a person lives, limit the places where a person can travel and can even dictate terms of employment. A breach of an order of this type can

[14] HM Government n.10, [2.37]
[15] Home Office, *New Powers Against Organised and Financial Crime* (CM 6875, July 2006) [2.4]

result in a maximum 5 year custodial sentence.[16] A further provision relates to data sharing between government organisations to tackle fraud.[17] For example the Act now allows for police forces to liaise with other organisations to help build evidence in fraud-related cases.

One of the biggest changes implemented under part 2 of the Serious Crime Act relates to inchoate offences. The purpose of part two of the Serious Crime Act is to '… allow people who assist another to commit an offence to be prosecuted regardless of whether the underlying substantive offence is actually committed or attempted.'[18] Essentially, the Serious Crime Act has codified the common law offence of incitement after concerns were raised that there was a gap in the law:

> '… [T]he common law does not recognise inchoate liability for assisting the commission of an offence if the offence is not subsequently committed or is committed without reference to [the defendants] assistance.'[19]

Under the original common law governing the encouragement of a crime, for an action to be brought before the courts it must have been found that the person who was encouraged to commit the criminal offence did carry out the act. The Serious Crime Act removes this condition, and therefore under this Act an individual can be liable for incitement where a further criminal offence has not taken place.

[16] Serious Crime Act 2007 Part 1 section 1
[17] Serious Crime Act 2007 Part 3
[18] The Crown Prosecution Service, 'Inchoate offences' (*CPS.gov*, 2017) <http://www.cps.gov.uk/legal/h_to_k/inchoate_offences/> accessed 3 November 2017
[19] Law Commission, *Inchoate liability for assisting and encouraging crime* (Law Com No 6878, 2006) [3.3]

Like that of the other provisions of the Act, the original purpose of this part of the Serious Crime Act was to target highly organised criminals:

> 'Under the common law, the police cannot proceed against D [defendant] until another person has committed or attempted to commit the principal offence. The lack of a general inchoate liability for assisting crime sits uneasily with the developments in intelligence-led policing which is now an important weapon in the state's response to serious organised crime.'[20]

Despite the need for the Serious Crime Act to remove the gaps in the common law, part two of the Act is considered to be '… fundamentally flawed'.[21] The Serious Crime Act is thought to have been drafted in an unnecessarily complex manner, an argument which reoccurs throughout the academic literature.[22] Originally, prosecutors were reluctant to charge individuals for offences contrary to the Serious Crime Act:

> 'I understood from informal discussions with some prosecutors that they thought that the offences would typically be avoided when determining appropriate charges, because they were considered to be too difficult to understand and to prosecute.'[23]

The reluctance of prosecutors to use the Serious Crime Act during its first few years, as Virgo exposed in his research, clearly indicates the lack of understanding in the criminal justice system as to when this Act should be utilised. Therefore, the Serious Crime Act breaches some of the key components of legality in the criminal law.

The principle of legality as explained in the chapter two upholds the idea that the law should be accessible. Accessibility simply means that the law needs

---

[20] *Ibid.,* [4.4]
[21] Graham Virgo, 'Part 2 of the Serious Crime Act 2007 - enough is enough' (2013) 3 Archbold Review 7
[22] *Ibid.,*
[23] *Ibid.,* 8

to be clear, an element that is lacking in the Serious Crime Act. In *Kafkaris v Cyprus*[24] the European Court of Human Rights stated that the law should be clear so that citizens can interpret legal rules, with the help of the courts if needed. The reluctance of law enforcers to use the Serious Crime Act, simply because they did not fully understand the law, meant that the law could never be fully interpreted. Yet the Serious Crime Act was used to prosecute several defendants in 2011, arising from their actions of encouraging other individuals to partake in criminal behaviour after riots broke out across the United Kingdom.

Following the shooting of Mark Duggan by armed police in London a demonstration was held outside Tottenham police station, which soon turned violent. Riots started to escalate all over the country with the use of violence, arson and theft taking place.[25] The disorder across the country lasted for five days and resulted in deaths, injuries and millions of pounds worth of property damage.[26] The level of destruction and outrage these actions caused brought many cases before the courts, with an emphasis being placed on stronger sentences to deter future offenders.[27] In several cases part two of the Serious Crime Act was used to prosecute defendants for their actions of

[24] *Kafkaris v Cyprus* App no 21906/04 (ECtHR, 12 February 2008)
[25] Vikram Dodd & Caroline Davies, 'London riots escalate as police battle for control' *The Guardian* (London, 9 August 2011) <https://www.theguardian.com/uk/2011/aug/08/london-riots-escalate-police-battle> accessed 3 November 2011
[26] Alexis Akwagyiram, 'England riots: One year on' *The BBC* (London, 6 August 2012) <http://www.bbc.co.uk/news/uk-19077349> accessed 3 November 2017
[27] Martin Beckford, 'London riots: Almost 1,000 jailed as judges give tougher sentences' *The Telegraph* (London, 22 February 2012) <http://www.telegraph.co.uk/news/uknews/crime/9101436/London-riots-Almost-1000-jailed-as-judges-give-tougher-sentences.html> accessed 21 January 2018

using the social media site, Facebook, to encourage others to participate in disorderly behaviour.

In *R v Jordan Blackshaw*[28] the defendant created a Facebook event page: 'Smash down in Northwich Town.'[29] The page was created on 8 August 2011, when riots were in full force across the country and being broadcasted worldwide. The event aimed to encourage individuals to start a riot in Northwich and included specific details as to when and where the riots would take place. As the page was made publicly available members of the local community quickly reported their concerns to the police, which resulted in Blackshaw later being arrested. As a result, the riot he attempted to organise never took place. He was charged and pleaded guilty to encouraging riots, burglary and criminal damage contrary to section 46 of the Serious Crime Act. He received a custodial sentence of four years which was later unsuccessfully appealed by his legal team.

In a similar case Sutcliffe-Keenan,[30] who under the influence of alcohol, used Facebook to create a public group page called 'The Warrington Riots'. The page included a photo of a police officer dressed in riot equipment in a 'standoff position' surrounded by a group of rioters and detailed a place to assemble in the Warrington area for the rioters to meet. Like that of

[28] *R v Jordan Blackshaw* Chester Crown Court 16 August 2011 (unreported)
[29] A Facebook event page is a resource used to notify other users of upcoming occasions. The page can be created privately, whereby the creator only invites specific users to the event or it can be open to the public for anyone to see. Facebook Events, 'Bring people together with Facebook Events' (*Facebook*, 2016) <https://events.fb.com/#events_landing_hero> accessed 3 November 2017
[30] *R v Perry Sutcliffe-Keenan* Chester Crown Court 16 August 2011 (unreported)

Blackshaw, the page was viewable to the public and was consequently reported to local police, resulting in the riot never taking place. Sutcliffe-Keenan was charged under section 44 of the Serious Crime Act, convicted and sentenced to four years imprisonment. His legal team also, unsuccessfully, appealed his sentence.

On 18 October 2011 the Court of Appeal heard 10 appeals related to the harsh sentences surrounding the United Kingdom riots, including the matters of *Blackshaw* and *Sutcliffe-Keenan*.[31] Though both cases were appealed on a number of grounds, one parallel reasoning concerned the disproportionate weight given by the judges in relation to deterrence. Deterrence is a punishment:

> '… imposed to make an example of conduct that has occurred or is alleged to have occurred. A system of general deterrence works on the assumption that there would be more stealing, more murder (to name only two offences) if warning examples of stealing or murder were not made by the imposition of punishment.'[32]

Under section 142(1) of the Criminal Justice Act 2003 it states that:

> '[a]ny court dealing with an offender in respect of his offence must have regard to the following purposes of sentencing- (a) the punishment of offenders, (b) the reduction of crime (including its reduction by deterrence), (c) the reform and rehabilitation of offenders, (d) the protection of the public, and (e) the making of reparation by offenders to persons affected by their offences.'

In *Blackshaw* and *Sutcliffe-Keenan* the Crown Court gave significant weight to the concept of deterrence, particularly following the public outcry for justice, and consequently the defendants were given increased sentences.[33]

---

[31] *Blackshaw* n.5
[32] Jim Morris, 'The structure of criminal law and deterrence' (1986) Aug Criminal Law Review 524, 525
[33] Carly Lightowlers & Hannah Quirk, 'The 2011 English "Riots": Prosecutorial Zeal and Judicial Abandon' (2015) 55(1) British Journal of Criminology 65

However, as discussed in chapter two, deterrence on its own can be considered as a flawed concept as it advocates the notion that criminal behaviour is thought out before taking place.

Despite the arguments that disproportionate sentences[34] were handed out following the disorder in August 2011, the Court of Appeal supported the use of the Serious Crime Act in *Blackshaw* and *Sutcliffe-Keenan*:

> 'We are unimpressed with the suggestion that in each case the appellant did no more than make the appropriate entry in his Facebook. Neither went from door to door looking for friends or like minded people to join up with him in the riot. All that is true. But modern technology has done away with the need for such direct personal communication. It can all be done through Facebook or other social media. In other words, the abuse of modern technology for criminal purposes extends to and includes incitement of very many people by a single step.'[35]

The Court of Appeal upheld the judgments of the Crown Court, despite the purpose of the Serious Crime Act being to target serious and organised crime. As previously specified the National Crime Agency and the Government define serious and organised crime as 'planned' and 'coordinated', two aspects missing from *Blackshaw* and *Sutcliffe-Keenan*. The aim of the Serious Crime Act was to target organised crime in England and Wales, with emphasis placed on the most serious of offences such as human trafficking and terrorism. However, part two of this Act was used to prosecute two defendants for committing social media related offences, which can be regarded as non-organised crime, and therefore goes against the purpose for which the Serious Crime Act was created.

---

[34] Frank Lowe (ed), 'The August 2011 Riots- Them and Us' in *Thinking Space: Promoting about Race, Culture, and Diversity in Psychotherapy and Beyond* (Karnac Books 2014) 226-227

[35] *Blackshaw* n.5, per Lord Judge CJ [73]

The use of this non-technology-based law to prosecute social media offences can be considered as an abuse of the law. Put simply, the actions undertaken by Blackshaw and Sutcliffe-Keenan was the creation of a Facebook event. The riots never took place, they did not physically contact others to become involved in the incident, and both defendants were under the influence of alcohol at the time the Facebook pages were created. This is supported further by Mitchell. Mitchell argues that the use of the Serious Crime Act and the case of *Blackshaw* leaves open the possibility of 'over-punishing' another,[36] a clear breach of the principle of legality. A precedent has now been set regarding those who encourage another to commit an offence *via* social media. In addition, in some cases individuals who were directly implicated in the riots had a lesser sentence imposed upon them,[37] creating inconsistencies in the legal system.

Under part two of the Serious Crime Act three unique situations of encouraging another to commit a criminal offence are prohibited. Both sections 44 and 45 have the same *actus reus*: 'A person commits an offence if he does an act capable of encouraging or assisting the commission of an offence.' In essence, the criminal conduct occurs when the defendant actively encourages another to partake in one singular criminal offence. For example, the use of social media to encourage a person to cause criminal

[36] Barry Mitchell, 'Sentencing riot-related offending: considering Blackshaw and others' (2011) 10 Archbold Review 4, 7
[37] Owen Bowcott, Haroon Siddique & Andrew Sparrow, 'Facebook cases trigger criticism of "disproportionate" riot sentences' *The Guardian* (London, 17 August 2011) <https://www.theguardian.com/uk/2011/aug/17/facebook-cases-criticism-riot-sentences> accessed 26 October 2016

damage to another's property would satisfy the *actus reus* under these two sections. Whereas the *mens rea* for both sections differ.

To bring an action under section 44 it must be found that the defendant intended to encourage a person to commit a criminal offence. As previously stated, there is no need for a further criminal act to occur as illustrated in *Sutcliffe-Keenan*. Whereas under section 45 the *mens rea* is one of belief. The Crown Prosecution Service (CPS) guidelines on inchoate offences state that the test for belief is similar to how the courts define belief in cases concerning stolen goods.[38] In *R v Edward Leonard Hall* belief is defined as:

> '… something short of knowledge. It may be said to be the state of mind of a person who says to himself: "I cannot say I know for certain that these goods are stolen, but there can be no other reasonable conclusion in the light of all the circumstances, in the light of all that I have heard and seen."'[39]

So, in relation to section 45, if it can be said that the defendant had a 'reasonable conclusion in light of the circumstances' that his actions may result in the encouragement of another to commit a criminal offence, he or she can be charged under section 45 of the Serious Crime Act.

It is not always clear when the Serious Crime Act will be used, or another Act of Parliament to criminalise actions conducted on social media sites. In 2017 Rhodri Phillips posted the following tweet: '£5,000 for the first person to "accidentally" run over this [Gina Miller] bloody troublesome first-generation immigrant.' Phillips posted the tweet following Gina Miller's legal case

[38] The Crown Prosecution Service n.18
[39] *R v Edward Leonard* Hall (1985) 81 Cr. App. R. 260 per Boreham J 264

against the Government regarding how Article 50 should be triggered, in order to start the proceedings of the United Kingdom leaving the European Union.[40] Following the decision of the High Court ruling in favour of Ms Miller, she was subjected to racist and sexist abuse online, including the comments above directed at Ms Miller from Phillips.[41]

The conduct of Phillips fulfils the *actus reus* of either section 44 or 45 of the Serious Crime Act: 'A person commits an offence if he does an act capable of encouraging or assisting the commission of an offence.' Though it may be difficult to prove intention under section 44 of the Act, it could have been possible to argue the *mens rea* of belief under section 45 of the Serious Crime Act. Yet Phillips was given a 12 week custodial sentence for sending a menacing communication contrary to section 127(1) of the Communications Act 2003, exposing inconsistencies within the law. Here, the law is not clear and therefore not accessible, providing further evidence that the Serious Crime Act does not comply with the principle of legality from a social media perspective.

Whereas sections 44 and 45 of the Serious Crime Act governs the encouragement of one singular criminal act, section 46 states: 'A person commits an offence if he does an act capable of encouraging or assisting the

[40] *R v Rhodri Phillips* Westminster Magistrates' Court 13 July 2017 (unreported). See also, Julia Gregory, 'Aristocrat faces jail after being menacing and racist about Gina Miller' *The Guardian* (London, 11 July 2017) <https://www.theguardian.com/uk-news/2017/jul/11/man-jail-offering-moneyrun-over-gina-miller-rhodri-philipps-viscount-brexit> accessed 20 July 2017.

[41] Lisa O'Carroll, 'Gina Miller: "I've been told that as a colored women, I'm not even human"' *The Guardian* (London, 25 January 2017) <https://www.theguardian.com/politics/2017/jan/25/parliament-alone-issovereign-gina-miller-speaks-out-after-article-50-victory> accessed 6 June 2017

commission of one or more of a number of offences.' This section governs the conduct of an individual encouraging another to commit more than one criminal offence. So, for instance in the case of *Blackshaw* it was found that he encouraged social media users to partake in riots, burglary and criminal damage. Like that of section 45, the *mens rea* is one of belief. The judgment of *Blackshaw*, though not sufficiently clear, indicated that to bring action under section 46 the prosecution did not have to prove the belief that each offence would take place, it was enough to prove a belief that at least one of the criminal acts may be committed. Whereas the Court of Appeal took a different approach in *R v Sadique and Hussain (No2).*[42]

Sadique was convicted of assisting in the supply of Class A and Class B drugs contrary to section 46 of the Serious Crime Act. He had sold several chemicals to another who utilised them to 'cut' these illegal substances. Though the selling of these chemicals was lawful, it was proven by the prosecution that Sadique reasonably understood that the chemicals would be used for illegal purposes. The question before the court concerned whether under section 46 Sadique needed to believe that all the offences would take place, or if it was satisfactory to prove belief in just one of the criminal acts. The court held, unlike the judges in *Blackshaw*, that all the offences needed to be established to bring action under section 46.

It is hard to clearly understand the difference between section 45 and 46 by applying the judgment of the court in *Sadique*. Here, under section 46 the

[42] *R v Sadique and Hussain (No2)* [2013] EWCA Crim 1150, [2013] 2 Cr. App. R. 31

prosecution would have to prove each offence separately, essentially fulfilling the *actus reus* and *mens rea* of section 45. As Child's argues section 46 has now been made redundant by the Court of Appeal.[43] This leaves issues with prosecuting social media related offences under the Serious Crime Act due to the lack of clarity as to when section 46 of the Act will apply over that of section 45, as both the legislation and the subsequent case law is unclear.

From an International Criminal Law perspective on legality, the law needs to be explicit, clear and beyond doubt.[44] The Serious Crime Act lacks the criteria of being explicit and clear. The judgments of *Blackshaw* and *Sadique* do very little to bring clarity to this Act of Parliament. Even from a more liberal approach as undertaken by the European Court of Human Rights,[45] the Serious Crime Act breaches the principles of accessibility and foreseeability in its use in prosecuting social media related offences.

In addition, the Serious Crime Act was intended to help tackle serious and organised crime. Yet its use in *Blackshaw* to prosecute two individuals for social media offences, which falls outside the Acts definition of serious crime, is a fundamental breach of the law. The conduct of the defendants was reckless, even stupid, but their encouragement of others to join in the riots

[43] John J Child, 'Exploring the mens rea requirements of the Serious Crime Act 2007 assisting and encouraging offences' (2012) 76(3) Journal of Criminal Law 220, 222
[44] *Čelebići Camp, Prosecutor v Delalić (Zejnil) and others,* Appeal Judgment, Case No IT-96-21-A, ICL 96 (ICTY 2001), 20th February 2001, United Nations Security Council [UNSC]; International Criminal Tribunal for the Former Yugoslavia [ICTY]; Appeals Chamber
[45] Darryl Robinson, *The Principle of Legality in International Criminal Law* (Legal Studies Research Papers Series 10-08, 2010) 5

never resulted in a further criminal offence taking place and both defendants were remorseful.

Whereas in the matter of *Phillips*, he was convicted under a lesser offence despite his actions being similar to Blackshaw and Sutcliffe-Keenan. Phillips actively encouraged others to commit a criminal offence, in this case the killing of Ms Miller in exchange for £5,000. Though his actions may not have fulfilled the *mens rea* of intent, it could be argued that the elements of belief were present in his conduct. Despite this, he was convicted under the Communications Act, which carries a significantly lower sentencing tariff in comparison with the Serious Crime Act.[46]

The use of the Serious Crime Act to prosecute social media offences is supported by the CPS in their guidelines on prosecuting communications sent *via* social media: 'Those who encourage others to commit a communications offence may be charged with encouraging an offence under the Serious Crime Act 2007.'[47] Here, the CPS supports the idea that if an individual encourages another, *via* the use of social media to commit a crime, they 'may be charged' contrary to the Serious Crime Act. The guidelines go further to indicate several online behaviours which may constitute an offence under the Act. For instance, they suggest that the conduct of 'virtual

[46] The maximum sentence under section 127 of the Communications Act 2003 is a 6 month custodial sentence. Whereas under the Serious Crime Act 2007 sections 44 to 46, the defendant is sentenced in line with the offence they had attempted to commit.
[47] The Crown Prosecution Service, 'Guidelines on prosecuting cases involving communications sent via social media' (*CPS.gov*, 2016) <https://www.cps.gov.uk/legal-guidance/guidelines-prosecuting-cases-involving-communications-sent-social-media> accessed 10 January 2018

mobbing', also commonly referred to as 'dogpiling', can be considered an offence under the Serious Crime Act, in certain circumstances. Virtual mobbing '… occurs when a number of individuals use social media or messaging to make comments about another individual ...'.[48]
If someone uses social media to encourage others to partake in this form of abuse, i.e. the virtual mobbing of another, this may well fall within the *actus reus* of section 44, 45 or 46 of the Serious Crime Act.

The CPS guidelines and the use of the Serious Crime Act in the context of social media can be considered as vague. The guidelines support the concept that the Act should be utilised when online communications are used to encourage others to commit a criminal offence but seems to go no further than this. There is a small list of online behaviours which may fall under the Serious Crime Act included in the guidelines, for instance virtual mobbing, the encouragement of derogatory hashtags and doxing (publishing a person's personal details), though little information is given as to how these apply in relation to the Serious Crime Act, except that encouragement is needed. This could be because there are currently no relevant case law examples to include in the guidelines.

Furthermore, how the Serious Crime Act is constructed has caused issues in itself:

> 'Having three new offences where only one would do creates complications not just in theory but in practice too, because it enables defendants to argue that they have been charged with the wrong one

[48] The Crown Prosecution Service, 'Cybercrime - Legal Guidance' (*CPS.gov*, 2018) <https://www.cps.gov.uk/legal-guidance/cybercrime-legal-guidance> accessed 10 January 2018

[incorrect offence] ...'.[49]

From the examination of case law examples and academic commentary, there is a lack of clarity when it comes to the use of the Serious Crime Act, particularly in a social media context. Though the courts have several fundamental roles, one important characteristic of the courts is to decide on legal disagreements, and in some instances creating the foundations for which future cases can be built. Nonetheless, matters prosecuted under the Serious Crime Act fail to give clear guidance for future disputes, especially where social media is concerned. This is a fundamental breach of the principle of legality. The Serious Crime Act is not accessible or foreseeable, and therefore constitutes a violation of this key legal notion.

Public Order Act 1986

Like that of the Serious Crime Act, the Public Order Act 1986 has been used to prosecute social media offences. The discussion below will outline the historical background of the Public Order Acts implementation into the legal system in England and Wales, before exploring in detail the *actus reus* and *mens rea* of part three, section 19 of the Act. By critically examining the use of the Public Order Act to prosecute social media related offences, issues will be exposed with the clarity of the Act and its use to govern technology-based criminal conduct.

[49] John Spencer & Graham Virgo, 'Encouraging and assisting crime: legislate in haste, repent at leisure' (2008) 9 Archbold News 7

During the early 1980s a rise in workplace demonstrations occurred across the United Kingdom, such as the Miners' Strike in 1984 which lasted for over a year.[50] In addition several riots, resulting in injuries, criminal damage and deaths occurred across England and Wales. On 28 September 1985 violence and disorder erupted in South London Brixton, following the accidental shooting of a woman by armed police, causing her serious injury.[51] The riots resulted in 13,758 burglaries and 53 individuals being hurt, one sustaining critical injuries.[52] A week later a further riot broke out in Tottenham following the death of a woman who suffered heart failure when police forced their way into her home. The disorder in Tottenham resulted in a police officer being stabbed to death.[53] Following the outbreak of these and other riots, the Conservative Government decided adequate legislation was needed to protect public safety and maintain public order,[54] reflecting elements of deterrence theory.

Public disorder is considered offences which disrupt a community and should be criminalised to keep the peace. It covers a range of scenarios including, though not limited to, football violence, riots and protests. Prior to the Public

[50] Christine Jeavans, 'The miners' darkest year' *The BBC* (London, 4 March 2004) <http://news.bbc.co.uk/1/hi/uk/3494024.stm> accessed 2 January 2018
[51] The BBC, 'On this day: 1985: Riots in Brixton after police shooting' *The BBC* (London, 2017) <http://news.bbc.co.uk/onthisday/hi/dates/stories/september/28/newsid_2540000/2540397.stm> accessed 2 January 2018
[52] Gareth Parry, Susan Tirbutt & David Rose, 'From the archive: Riots in Brixton after police shooting' *The Guardian* (London, 30 September 1985) <https://www.theguardian.com/theguardian/2009/sep/30/brixton-riots-1985-archive> accessed 2 January 2018
[53] The BBC, 'What caused the 1985 Tottenham Broadwater Farm riot?' *The BBC* (London, 3 March 2014) <http://www.bbc.co.uk/news/uk-england-london-26362633> accessed 2 January 2018
[54] Jim Driscoll, 'Protest and Public Order: The Public Order Act 1986' (1987) Sep Journal of Social Welfare Law 280

Order Act receiving Royal Assent, public order offences were controlled under several Acts of Parliament, including the Public Order Act 1936. The 1936 Act was enacted by Parliament to control political marches during the 1930s. Under the 1936 Act, the police had limited powers to contain political marches.[55] For instance, under section 3 of the Public Order Act 1936 the police could only impose conditions on marches when public disorder was at risk. Following the enactment of the 1936 Act, the police had to rely on other Acts to maintain order including, the Criminal Justice Act 1982 and the Sporting Events (Control of Alcohol ect) Act 1985. However, neither of these Acts gave the police significant power to control public disorder, resulting in a new Act being created: the Public Order Act 1986.

The purpose of the 1986 Act was:

> '… to abolish the common law offences of riot, rout, unlawful assembly and affray and certain statutory offences relating to public order; to create new offences relating to public order; to control public processions and assemblies; to control the stirring up of racial hatred …'.[56]

The Act was seen to have two objectives. First to '… provide a comprehensive code as to the organisation and control of processions and demonstrations'.[57] Second, to create a code relating to disorderly conduct, essentially codifying parts of the common law. The Act also introduced new offences such as controlling racial hatred. It was 'aimed at protecting those in … communities who [were] most vulnerable to loutish and abusive

[55] Andrew Beale, *Essential Constitutional Law* (2nd edn, Cavendish Publishing Limited 1997) 83
[56] Public Order Act 1986
[57] Hilaire Barnett, *Constitutional & Administrative Law* (12th edn, Routledge 2017) 524

behaviour- particularly the elderly.'[58] Yet twenty-six years later part three of the Public Order Act was utilised to control racial hatred aided by social media.

Part three of the Public Order Act criminalises the behaviour of 'racial hatred.' Racial hatred is considered '… hatred against a group of persons … defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins.'[59] A literal approach should not be used when it comes to 'race', words such as 'African, foreigners and immigrants' can fall within the definition of race.[60] In *R v Martin Hartshorn*[61] it was held that the use of the word 'Paki' amounted to racial hatred and constituted a breach of part three, section 19 of the Public Order Act.

Section 19(1) makes it a criminal offence to publish:

> '… written material which is threatening, abusive or insulting … [which she/he] intends thereby to stir up racial hatred, or having regard to all circumstances racial hatred is likely to be stirred up ...'.

The *actus reus* is in the publication of the written material which is either threatening, abusive or insulting. These words will take their 'ordinary English meaning.'[62] Whereas the *mens rea* is one of intention or recklessness. It is

[58] HC Deb 13 January 1986, vol 89, cols 792-869, 793
[59] Public Order Act 1986 Part 3 section 17
[60] The Crown Prosecution Service, 'Violent Extremism and Related Criminal Offences' (*CPS.gov*, 2017) <https://www.cps.gov.uk/publications/prosecution/cases_of_inciting_racial_and_religious_hatred_and_hatred_based_upon_sexual_orientation.html> accessed 22 October 2017
[61] *R v Martin Hartshorn* Grimsby Crown Court 4 November 2011 (unreported). See also, Dave Higgens, 'Man jailed for riot race-hate posts' *The Independent* (London, 4 November 2011) <http://www.independent.co.uk/news/uk/crime/man-jailed-for-riot-race-hate-posts-6257282.html> accessed 22 October 2017
[62] The Crown Prosecution Service, 'Racist and Religious Hate Crime - Prosecution Guidance' (*CPS.gov*, 2017)

important to note that under section 19(2) of the Public Order Act a defence is available:

> '… it is a defence for an accused who is not shown to have intended to stir up racial hatred to prove that he was not aware of the content of the material and did not suspect, and had no reason to suspect, that it was threatening, abusive or insulting.'

Therefore, if the defendant can prove that he lacked the intent to cause racial hatred, he or she will not have committed an offence under section 19 of the Public Order Act.

Consequently, section 19 of the Public Order Act requires several factors to be established. First, the conduct in question needs to be 'threatening, abusive or insulting.' As previously stated, these words take their 'ordinary English meaning' and are a question based on fact. In addition, the conduct does not have to fall under all three categories, one is sufficient. Next, racial hatred needs to be established using the definition found under part three, section 17 of the Act. Here, 'race' and 'hatred' are segregated.[63] Last, the conduct needs to stir up racial hatred or considered likely to stir up this type of behaviour. The term likely is defined as '… more than merely possible or likely.'[64] If these factors can be established and the defence under section 19(2) is disproven, then a breach of section 19 of the Public Order Act has occurred.

<http://www.cps.gov.uk/legal/p_to_r/racist_and_religious_crime/#a07> accessed 22 October 2017

[63] The Crown Prosecution Service n.60

[64] *Ibid.,*

During parliamentary discussions before the enactment of the Public Order Act the inclusion of racial hatred was praised:

> 'I welcome especially the clause dealing with incitement to racial hatred. I strongly believe that people of every race and colour deserve the protection of the law against racial abuse and the kind of hate campaigns that some hon Members, especially those from inner London, know what can occur. It is right to give reasonable protection to all sections of the community.'[65]

In the 1970s and early 1980s racial hatred was very much apparent in society.[66] Several demonstrations were held by National Front, a far-right political party, who opposed non-British nationals. These demonstrations and marches would often occur through ethnic minority areas and in some cases turned violent.[67] In 1977 disorder erupted in Lewisham South London, following National Front marching through the town in response to ethnic minorities living in the area. Overall 111 people were injured during the incident and 241 individuals were arrested.[68] The growing racial tension and the need to criminalise this behaviour was the rationale behind its inclusion in the Public Order Act:

> 'There is a problem of racism in Britain - a desperately serious one - and it is one to which we must address ourselves. At times of economic distress there is a search for scapegoats, and scapegoats are often minority ethnic groups.'[69]

[65] HC Deb 13 January 1986 n.58
[66] Nathan Hall, *Hate Crime* (2nd edn, Routledge 2013) 33
[67] Ben Bowling & Coretta Phillips, 'Racist Victimisation in England and Wales' in Darnell F. Hawkins (ed), *Violent Crime: Assessing Race and Ethnic Differences* (Cambridge University Press 2003) 165
[68] Mark Townsend, 'How the battle of Lewisham helped to halt the rise of Britain's far right' *The Guardian* (London, 13 August 2017) <https://www.theguardian.com/uk-news/2017/aug/13/battle-of-lewisham-national-front-1977-far-right-london-police> accessed 10 January 2018
[69] HC Deb 13 January 1986 n.58, 857

The Public Order Act was considered an opportunity to strengthen the law. The purpose, like that of the overall aim of the Act, was to help restore public order, yet it has since been used to govern social media related offences.[70]

In 2012 Liam Stacey was convicted and sentenced to fifty-six days in jail for sending racist and obscene tweets, following the collapse of Bolton Wanderers star Fabrice Muamba during a football match.[71] On 17 March 2012 Muamba went into cardiac arrest whilst playing in a football match against Tottenham Hotspurs, which was being broadcasted live on television. For six minutes medical staff helped to resuscitate him on the pitch.[72]

Following the incident, Stacey, who was a student at Swansea University, took to his personal Twitter page to make several racist comments about Muamba including: 'LOL [Laughing out Loud]. Fuck Muamba he's dead [*sic*]!!! #Haha' and 'Go suck a nigger [*sic*] dick you fucking aids-ridden cunt.' Stacey made numerous tweets of this nature not only aimed at Muamba but also other individuals who attempted to defend the footballer.[73] His behaviour resulted in several complaints being made to the police. Stacey was later arrested and convicted under the Public Order Act.

[70] For instance, *R v Sheppard and Whittle* [2010] EWCA Crim 65
[71] *R V Liam Stacey* Swansea Crown Court On Appeal From The Magistrates' Court A20120033. Note, Stacey was prosecuted under section 31(1)(b) of the Public Order Act.
[72] BBC Sport, 'Bolton's Fabrice Muamba collapses during Spurs-Bolton match' *The BBC* (London, 17 March 2012) <http://www.bbc.co.uk/sport/football/17417973> accessed 10 January 2018
[73] Steven Morris, 'Student jailed for racist Fabrice Muamba tweets' *The Guardian* (London, 27 March 2012) <https://www.theguardian.com/uk/2012/mar/27/student-jailed-fabrice-muamba-tweets> accessed 10 January 2018

The use of the Public Order Act to prosecute social media related offences has created a divide amongst academic researchers. Dorfman rejects the idea that this law should be used when it comes to social media, especially when there is no element of violence present:

> '… [U]sing the Public Order Act for a few nasty Twitter comments which never advocated violence or hatred against specific people is a downright abuse of the law; at no time was "public order" ever threatened in any reasonable conception of the term.'[74]

Dorfman argues that the conduct of *Stacey* lacks the relevant criteria needed to prosecute an individual under the Public Order Act, despite Stacey's successful conviction. Though the behaviour of the defendant was abusive and had a racial element, his actions did not stir up racial hatred nor could it be said that it was likely to cause racial hatred.

Stacey's behaviour was abusive but at no point can it be said that there was a threat to public order. In *Dehal v Crown Prosecution Service* Moses J stated when referring to section 4A of the Public Order Act, that:

> '… the criminal law should not be invoked unless and until it is established that the conduct which is the subject of the charge amounts to such a threat to public order as to require the invocation of the criminal as opposed to the civil law.'[75]

This is supported further in the CPS guidelines on social media related offences:

> '… [P]articular care should be taken in dealing with social media cases in this way because public order legislation is primarily concerned with words spoken or actions carried out in the presence or hearing of the person being targeted (i.e. where there is physical

[74] Rosalee Dorfman, 'Can you say "social media prosecutions" with a straight face? The Crown Prosecution Service can' (2013) The Leeds Journal of Law and Criminology <http://criminology.leeds.ac.uk/2013/09/05/social-media-prosecutions/> accessed 20 October 2016

[75] *Dehal v Crown Prosecution Service* [2005] EWHC 2154 per Moses J [5]

proximity between the speaker and the listener) …'.[76]

The CPS upholds the idea that the Public Order Act should only be used in limited circumstances, but it is not clear from the guidelines what constitutes these conditions. The guidelines mention the difference between 'irritating, contentious, unwelcome and provocative' conduct and behaviour that provokes violence, though no clarity is given beyond this.

It could be said that the law has adapted to the changing nature of society, by allowing the Public Order Act to criminalise conduct carried out online. The adaptation of the law to fit the changing circumstances of a given society conforms to the principle of legality as affirmed in *SW and CR v United Kingdom*,[77] so long as the change is foreseeable. The *actus reus* of the Public Order Act states that the conduct must incite public disorder as public order is considered a 'fundamental social good.'[78] Whereas public disorder affects the social wellbeing of a society, this was reflected in the tough stance taken by Parliament during the implementation of the Public Order Act:

> 'The 1986 Act like its predecessor is very much a pragmatic reaction to recent events. It was passed against the background of inner-city disturbances, soccer hooliganism, racist marches and racist attacks on members of the ethnic minorities, mass industrial picketing and the resurgence of major public demonstrations. The Act is not founded on well articulated premises addressing the scope and ambit of the criminal law in the area of public order.'[79]

[76] The Crown Prosecution Service n.47
[77] *SW v United Kingdom, CR v United Kingdom* App no 20166/92 (ECtHR, 22 November 1995)
[78] HC Deb 13 January 1986 n.58, 792
[79] Driscoll n.54

The purpose of the Public Order Act was to regulate public disorder in particular, riots, football hooliganism and protests which were very much apparent during the early 1980s, an element missing in the matter of *Stacey*. Yet the Act has been used to cover social media related offences, despite the Public Order Act being enacted 20 years before Twitter was made available to the public. For Haralambous and Geach this is a clear breach of the rule of law, and consequently undermines the principle of legality in the criminal law.[80]

As explained previously the rule of law consists of several key principles: no individual, regardless of status is above the law, the Government must act lawfully, and the law should be applied equally to all those living in a society.[81] Though there are many theories and approaches to the rule of law, those that take a substantive approach[82] argue that the law should be explicit and therefore certain: '… [T]he law must be accessible and so far as possible intelligible, clear and predictable …',[83] arguably two areas missing regarding the use of the Public Order Act in a social media context.

The purpose of the Public Order Act was to maintain public order during a time when demonstrations were on the rise. Despite the purpose of the Act, the Public Order Act has since been used to prosecute conduct carried out

[80] Nicola Haralambous & Neal Geach, 'Online Harassment and Public *Dis*-order' (2010) 174 Criminal Law and Justice Weekly 409, 411
[81] Mark Elliot & Robert Thomas, *Public Law* (3rd edn, Oxford University Press 2017) 65
[82] There are two opposing theoretical positions when it comes to the rule of law: procedural and substantive. Those that take a procedural approach argue that so long as the law has been enacted in the correct manner, the law should stand. Whereas substantive theorists argue that the substance of the law needs to be taken into account. See, Paul Craig, 'Formal and substantive conceptions of the rule of law: an analytical' (1997) Public Law 467
[83] Lord Bingham, 'The rule of law' (2007) 66(1) Cambridge Law Review 67, 69-70

on social media, however its use is unclear. For instance, the Public Order Act was applied in *Stacey* but not in the matter of *R v Alison Chabloz*.[84]

Chabloz uploaded several YouTube video's online mocking Holocaust victims and survivors, including Anne Frank. In these videos she also made 'expressions of anti-Semitic hatred'.[85] It was put before the court that her actions were '… designed to provoke maximum upset and discomfort ...'.[86] Despite this, she was convicted for sending grossly offensive material *via* a communications network contrary to section 127(1) of the Communications Act 2003, even though her actions, by applying the case of *Stacey,* indicate a breach of the Public Order Act.

Stacey and *Chabloz* can both be considered abusive in their content and demonstrates racial hatred. Stacey used the phrase, 'go suck a nigger [*sic*] dick you fucking aids-ridden cunt.' Chabloz used several anti-Semitic terms, including comparing Auschwitz concentration camp to '… a theme park just for fools.' The main issue falls on whether the behaviour of both defendants was likely to stir up racial hatred. In *Stacey* the CPS concluded that this was the case, though this is not fully accepted in the academic literature.[87] Whereas in *Chabloz* it is unclear if this was considered by the CPS as charges were brought under a different Act of Parliament. If the rationale of

[84] *R v Alison Chabloz* Westminster Magistrates' Court 11 January 2018 (unreported). For more information on this case, see chapter six.
[85] ITV News, 'Blogger "mocked Anne Frank and Holocaust survivors" court told' *ITV News* (London, 11 January 2018) <http://www.itv.com/news/2018-01-11/blogger-mocked-anne-frank-and-holocaust-survivors-court-told/> accessed 11 January 2018
[86] *Ibid.,*
[87] Dorfman n.74

Stacey is applied, it is hard to distinguish why Chabloz was not prosecuted for a breach of section 19 of the Public Order Act. This is even more apparent as during the hearing held at Westminsters' Magistrates Court, one of Chabloz's videos was played, which was met with a round-of-applause by supporters in the public gallery.[88] Arguably, the Public Order Act fails to uphold the key principles of legality, as it is uncertain when this Act will be used in a social media context, as there is a lack of consistency as to when the CPS will press charges under the Public Order Act for social media related offences.

There is also the potential that a further section of the Public Order Act can be used in relation to online abuse, which is currently not being fully utilised. Section 4A[89] of the Public Order Act makes it an offence to cause a person harassment, alarm or distress with intent by using:

> '… threatening, abusive or insulting words or behaviour, or disorderly behaviour, or displays any writing, sign or other visible representation which is threatening, abusive or insulting.'[90]

Like that of section 19 covering racial hatred, this section was included in the Public Order Act to help combat the issue of race-related crime. Section 4A could be applied to criminalise the conduct of online harassment, commonly referred to as cyber harassment:

> 'Online harassment refers to the sending of repeated threatening or harassing electronic communications *via* email, websites, or other digital media that cause another person to be harmed or deeply

[88] ITV News n.85
[89] Section 4A was implemented into the Public Order Act 1986 by the Criminal Justice and Public Order Act 1994 section 154
[90] Public Order Act 4A(1)

disturbed.'[91]

Though cyber harassment can fall under the Protection from Harassment Act 1997, as discussed in the following section, the Public Order Act provides key advantages over that of the Protection from Harassment Act.

Under the Public Order Act 'harassment', 'alarm' and 'distress' are deemed to have separate and distinct meanings:

> 'Harassment, alarm and distress do not have the same meaning. One can be harassed, even seriously harassed, without experiencing emotional disturbance or upset at all. However, although the harassment does not have to be grave, it should not be trivial. The court has to find that the words or behaviour were likely to cause some real, as opposed to trivial, harassment.'[92]

Subsequently, it is sufficient if only harassment can be proven in a case, there is no need for alarm or distress to be present, elements needed for a successful conviction under the Protection from Harassment Act.[93] Furthermore, under the Public Order Act, harassment is not specifically defined and therefore a course of conduct does not need to be present. An aspect which is needed when bringing an action under the Protection from Harassment Act as discussed in the following section.

Social media has created new and unique ways in which an individual can harass and torment another, for instance 'online mobbing'.[94] As previously stated online mobbing is where someone is attacked or abused online

---

[91] Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime* (2nd edn, Routledge 2011) 129
[92] *Southard v Director of Public Prosecutions* [2006] EWHC 3349 (Admin), [2007] A.C.D. 53 per Latham L.J. and Fulford J [10]
[93] Discussed in detail in later parts of this chapter.
[94] Danielle Keats Citron, 'Cyber Civil Rights' (2008) 89 Boston Law Review 61

continuously by a group of individuals.[95] Jess Phillips a Labour MP for Birmingham Yardley, has publicly spoken about receiving more than 600 rape and death threats in one night alone *via* Twitter.[96] Many of these comments came from different individuals rather than the same person. Though this conduct would fall under the definition of online mobbing, by applying the definition of harassment under the Protection from Harassment Act, this type of behaviour may not be successfully criminalised under the Act. However, it could fall under the Public Order Act. Subsequently, the Public Order Act is not being used to its full advantage.

Despite this, the social media guidelines implemented by the CPS, support the idea of the Public Order Act being used to prosecute certain specific online behaviours, which have emerged since the revolution of the Internet. For instance, the creation of false or offensive social media profiles. In *S v Crown Prosecution Service*[97] an individual uploaded an image online of a security guard, who worked at an animal testing facility. The image had been altered to encompass a speech bubble with false information contained within it.[98] The defendant was successfully convicted under section 4A of the

[95] Debarati Halder & Karuppannan Jaishankar, 'Cyber Socializing and Victimization of Women' (2009) *TEMIDA* 5, 12 <http://www.doiserbia.nb.rs/img/doi/1450-6637/2009/1450-66370903005H.pdf> accessed 25 October 2017
[96] Sally Hayden, 'Labour's Jess Phillips received "600 rape and death threats in a single day"' *The Independent* (London, 27 August 2017) <http://www.independent.co.uk/news/uk/home-news/labour-mp-jess-phillips-rape-death-threats-one-day-social-media-attacks-training-a7915406.html> accessed 25 October 2017
[97] *S v Crown Prosecution Service* [2008] EWHC 438
[98] For instance, one comment stated that the security guard had been convicted for a violent crime in the past.

Public Order Act for causing another person harassment, alarm or distress by displaying writing which was abusive and insulting.[99]

Though section 4A of the Public Order Act could be used more effectively to tackle online abuse, the main issue regards the Acts lack of clarity. Like that of the Serious Crime Act, the use of the Public Order Act in a social media context can be seen as a serious breach of the rule of law, and therefore does not conform to the principle of legality. The purpose of the Act was to maintain public disorder, not to prosecute social media related offences.

The discussion above illustrates the difficulties in establishing when the Public Order Act will be used to prosecute a social media offence or when another Act of Parliament will take precedence, for instance the Communications Act. This brings issues with understanding when the Public Order Act will be used in a social media context, especially where online abuse is concerned. This leaves two possibilities: victims of online abuse being let down by the system, as law enforcers fail to apply the appropriate legislation, or abusers being prosecuted and convicted under the wrong Act of Parliament.

[99] David Barrett, 'Faking social media accounts could lead to criminal charges' *The Telegraph* (London, 3 March 2016) <http://www.telegraph.co.uk/news/uknews/crime/12180782/Faking-social-media-accounts-could-lead-to-criminal-charges.html> accessed 11 January 2018

Protection from Harassment Act 1997[100]

The purpose of the Protection from Harassment Act 1997 is to 'protect the victims of harassment … [including from] … so-called stalking behaviour, racial harassment, or anti-social behaviour by neighbours.'[101] A report undertaken by the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate in 2017, exposed a lack of understanding across the criminal justice system when it came to the use of the Protection from Harassment Act. [102] The following discussion will start by defining the difference between harassment and stalking, before critically evaluating each behaviour separately. Here, the *actus reus* and *mens rea* of the offence will be explained, before examining its use in a social media context.

It has been widely accepted that the Protection from Harassment Act covers the conduct of harassment and stalking online.[103] Harassment is considered:

> '… repeated attempts to impose unwanted communications and contact upon a victim in a manner that could be expected to cause distress or fear in any reasonable person.'[104]

[100] Part of this section has been published in the Journal of Criminal Law. See, Laura Bliss, 'The Protection from Harassment Act 1997: Failures by the Criminal Justice System in a Social Media Age' (2019) 83(3) Journal of Criminal Law 217
[101] HL Deb 24 January 1997, vol 1, col 917
[102] Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate, 'Living in fear – the police and CPS response to harassment and stalking' (*justiceinspectorates.gov*, July 2017) 15 <http://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/living-in-fear-the-police-and-cps-response-to-harassment-and-stalking.pdf> accessed 29 November 2017
[103] When the Act was originally enacted in 1997 harassment and stalking were considered as one offence. However, in 2012 under the Protection of Freedoms Act 2012 section 111(1), stalking was included in the Protection from Harassment Act as a separate offence.
[104] The Crown Prosecution Service, 'Stalking and Harassment' (*CPS.gov*, 2017) <http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/> accessed 10 November 2017

Whereas stalking is 'a constellation of behaviours in which one individual inflicts on another repeated unwanted intrusions and communications.'[105] Under section 2A(3) of the Protection from Harassment Act examples of conduct that would amount to stalking have been listed. For instance:

> '… following a person … monitoring the use by a person of the Internet, email or any other form of electronic communication … [and] watching or spying on a person'.

Prior to the 1997 Act coming into force the conduct of both stalking and harassment were governed under several Acts of Parliament in England and Wales, including the Malicious Communications Act 1988, the Telecommunications Act 1984, the Public Order Act 1986 and the Offences Against the Person Act 1861,[106] demonstrated in *Regina Respondent v Ireland Appellant*.[107] The defendant made several malicious phone calls to the complainant over a period of three months. This case came before the courts prior to the enactment of the Protection from Harassment Act. As a result, the court extended the definition of assault and actual bodily harm under the Offences Against the Person Act. Here, the House of Lords came to the opinion that the conduct of silence could amount to an assault and psychiatric injury contrary to section 20 of the Offences Against the Person Act.

Despite the successful conviction in *Ireland*, during a Home Office consultation committee examining stalking, it was concluded that the criminal

[105] Michele Pathé & Paul Mullen, 'The impact of stalkers on their victims' (1997) 170(1) The British Journal of Psychiatry 12
[106] Mary Baber & Helena Jeffs, Stalking, harassment and intimidation and the Protection from Harassment Bill (Research Paper 96/115, 13 December 1996) 5-6
[107] *Regina Respondent v Ireland Appellant* [1997] 3 W.L.R. 534, [1998] A.C. 147

law was inadequate when it came to protecting individuals from this form of abuse:

> 'Though the offences under the Public Order Act may provide a sanction against stalkers in some instances, offences under the provisions of sections 4 and 4A would be committed only if the stalker intended his behaviour to cause the victim to believe that immediate violence would be used (section 4) or if harassment, alarm or distress is caused (section 4A). There are problems also in applying other aspects of the criminal law against stalkers. The Malicious Communications Act 1988 requires that the article sent must be indecent or grossly offensive. It must also be proved that the sender's purpose was to cause distress or anxiety. In the situations where stalkers continually send greetings cards, flowers or other unsolicited gifts, such intent cannot be proven.'[108]

Furthermore, the variety of Acts available to prosecute individuals for harassment and stalking behaviours has resulted in failures by the criminal justice system to adequately protect victims from this type of conduct.[109]

Evonne Van Heussen, who was the founder of the National Anti-Stalking and Harassment Support Association,[110] was stalked for a total of 17 years by a man she barely even knew between 1975 and 1991.[111] Between 1975 and 1978 she was subjected to mysterious silent phone calls, dead flowers being left outside her home and photographs of herself and her children being posted through her letterbox. During the first three years Ms Van Heussen did not know who was behind the conduct. In 1978 the man responsible broke into her house. He held her hostage for eight hours, where he attempted to rape her before a neighbour heard her screams and alerted the

[108] Home Office, *Stalking A Consultation Paper* (11 July 1996) [3.4-3.6]
[109] Emma Cook, 'Harassed relentlessly by a stranger, Evonne von Heussen formed an anti-stalking group. Emma Cook reports' *The Independent* (London, 22 January 1995) <http://www.independent.co.uk/life-style/stalked-for-years-by-a-man-she-met-once-1569160.html> accessed 4 January 2018
[110] Note this organisation no longer exists.
[111] Cook n.109

police. Despite Ms Van Heussen only recognising the man as her lecturer from two lectures she had attended a few years earlier, the police labelled the incident as a domestic issue, resulting in the defendant receiving a caution. He continued to stalk her for another thirteen years until Ms Van Heussen left the country.

Following stories like Ms Van Heussen's, and further pressure being placed on the Government for a change in the law by pressure groups such as the Suzy Lamplugh Trust, in late 1996 the Conservative Government presented an anti-stalking Bill. The Bill was first introduced into the House of Commons on 5 December 1996 and received Royal Assent on 21 March 1997. The Bill was rushed through Parliament by the Conservative Government to prove to voters, as at the time a General Election was due to take place, that the Government was being tough on crime.[112] Consequently, the original Act treated stalking and harassment as the same offence, this was amended in 2012.[113]

Stalking and harassment are not always easy to distinguish. Academic commentary tends to group these types of behaviours together. However, stalking and harassment carry different sentencing tariffs and police powers, therefore they must be considered separately.[114] For the purpose of this discussion, harassment and stalking will be critically examined in separate

[112] Judith Gowland, 'Protection from Harassment Act 1997: the "new" stalking offences' (2013) 77(5) Journal of Criminal Law 387
[113] Protection of Freedoms Act 2012 section 111(1)
[114] For example, under the Protection from Harassment Act for stalking offences the police have the power to enter and search property under section 2B.

subsections, before evaluating the current difficulties in prosecuting these two offences.

Harassment

Although harassment is defined within the Protection from Harassment Act, the wording of the Act is considered to be extremely wide, and as a consequence it can be used to govern online behaviour, commonly referred to as cyber harassment.[115] Cyber harassment as stated previously is the use of technology to impose unwanted contact upon another person.

Section 1 of the Protection from Harassment Act prohibits[116]: '… a course of conduct which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.'[117] Section 2 of the Act, makes it a criminal offence to harass another. The *actus reus* consists of two elements: a course of conduct and harassment. Following an amendment to the Protection from Harassment Act by the Serious Organised Crime and Police Act 2005, a course of conduct is defined as contact on at least two occasions.[118] However, from an examination of the case law, it is unlikely to

[115] Neal Geach & Nicola Haralambous, 'Regulating harassment: is the law fit for the social networking age?' (2009) 73(3) Journal of Criminal Law 241

[116] Section 2 of the Protection from Harassment Act outlines that a course of conduct is a criminal offence under the law.

[117] A further offence of harassment is governed under section 4 of the Protection from Harassment Act- putting someone in fear of violence. This has the same *actus reus* and *mens rea* as section 1 of the Act. However, if it can be found that the defendant 'knew or ought to know' that their behaviour would cause fear of violence in another, then they will be prosecuted under section 4. Here, the court has higher sentencing powers compared to that of section 1.

[118] The Protection from Harassment Act 1999 7(3). This was substituted into the Act by the Serious Organised Crime and Police Act 2005. The law treats a course of conduct differently, if multiple individuals are involved. Section 7(3)(b) 'in the case of conduct in relation to two or more persons … [a course of conduct is considered] … conduct on at least one occasion in relation to each of those persons.'

be found that a course of conduct would be present where only two instances have occurred:

> 'I fully accept that the incidents which need to be proved in relation to harassment need not exceed two incidents, but, as it seems to me, the fewer the occasions and the wider they are spread the less likely it would be that a finding of harassment can reasonably be made.'[119]

A minimum requirement has been set by Parliament as to when certain behaviours may invoke the Protection from Harassment Act. In most circumstances for the criminal justice system to be satisfied that a course of conduct is present in a matter, contact must occur on more than two occasions. This is a similar argument made by Agate and Ledward. They suggest that in most circumstances a course of conduct will only be established if it occurs on more than two occasions, which would need to be close in terms of time, despite the definition contained in the Act.[120] Little information can be gathered from the case law, the CPS prosecuting guidelines or academic commentary regarding what would constitute a close connection with reference to time. This leaves many questions unanswered when it comes to prosecuting harassment conducted online. For example, could it be said that contact once a month over the course of a year can amount to harassment, or would it need to be more contact over a shorter period of time?

---

[119] *Lau v Director of Public Prosecutions* [2000] 1 F.L.R 799 (DC) per Mr Justice Schiemann [15]

[120] Jennifer Agate & Jocelyn Ledward, 'Social media: how the net is closing in on cyber bullies' (2013) 24(8) Entertainment Law Review 263, 266. It is important to note that under section 1(3) of the Protection from Harassment Act, there is a defence available with regard to 'a course of conduct': '… (a) that it was pursued for the purpose of preventing or detecting crime, (b) that it was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under any enactment, (c) or that in the particular circumstances the pursuit of the course of conduct was reasonable.'

The second part of the *actus reus* is to establish harassment. Under the Protection from Harassment Act harassment is defined as 'alarming' a person or causing them 'distress'.[121] If from the evidence provided it can be established that the complained about behaviour amounts to alarming or distressing a person, the condition of harassment will be satisfied:

> 'Where the quality of the conduct said to constitute harassment is being examined, courts will have in mind that irritations, annoyances, even a measure of upset, arise at times in everybody's day-to-day dealings with other people. Courts are well able to recognise the boundary between conduct which is unattractive, even unreasonable, and conduct which is oppressive and unacceptable. To cross the boundary from the regrettable to the unacceptable the gravity of the misconduct must be of an order which would sustain criminal liability …'.[122]

This has created issues when it comes to the prosecution of harassment in a social media situation. In many cases of online harassment the conduct is 'disturbing, unpleasant and may transgress the norms of socially acceptable' behaviour, but it is difficult to prove that the conduct crosses a line to warrant criminal law intervention under the Protection from Harassment Act.[123] For example, the abuse inflicted upon Laura Bates a feminist writer, campaigner and political activist.

After Ms Bates started her online campaign, 'The Everyday Sexism Project', aimed at exposing the sexist attitudes that still exist in society today, she found herself on the receiving end of abusive online messages:

> 'Within a month of starting the project I was getting 200 messages everyday of really, really bad abuse … Really graphic descriptions of

[121] Protection from Harassment Act 1997 section 7(2)
[122] *Majrowski v Guy's and St Thomas's NHS Trust* [2006] UKHL 34, [2007] 1 A.C. 224 per Lord Nicolls of Birkenhead [30]
[123] Michael Salter & Chris Bryden, 'I can see you: harassment and stalking on the Internet' (2009) 18(2) Information & Communications Technology Law 99, 103

domestic violence and rape.'[124]

The receiving of these comments by Ms Bates will have no doubt been 'disturbing' and 'unpleasant', but without a course of conduct that amounted to harassment, it would have been difficult to prosecute an individual contrary to the Protection from Harassment Act.

The *mens rea* for the criminalisation of harassment is based on the construction of knowledge. Under the Protection from Harassment Act in order to bring a successful prosecution for harassment it must be proven that the defendant, 'knows or ought to know that the[ir] behaviour would amount to [the] harassment of another.'[125] The concept of 'knowledge' is based on the reasonable person test.[126] Essentially, it must be established that the average sober person in the same position as the defendant would come to the knowledge or should have come to the knowledge, that their conduct would amount to the harassment of another individual. If both the *actus reus* and *mens rea* of the offence can be found, then the defendant is liable for a breach of section 2 of the Protection from Harassment Act.

The anonymity of the Internet has made it easier for harassment to be conducted, as few security questions need to be answered to set up a social media profile.[127] For instance, to create a Facebook account the user merely

[124] Rebecca Holman, '"I've had death and rape threats simply for starting the conversation about everyday sexism"' (*The Debrief*, 30 April 2014) <https://thedebrief.co.uk/news/opinion/ve-death-rape-threats-simply-starting-conversation-everyday-sexism/> accessed 12 January 2018
[125] Protection from Harassment Act 1997 section 1(1)(b)
[126] For a discussion on the reasonable person see, Reid Griffith Fontaine, *The Mind of the Criminal: The Role of Developmental Social Cognition in Criminal Defense Law* (Cambridge University Press 2012) 13
[127] Salter & Bryden n.123

needs an email address as all other questions can be answered using an alias.[128] Consequently, social media has become a relatively new way to harass another.[129] However, there are issues with a lack of understanding by police forces and the CPS as to when the Protection from Harassment Act should be used to prosecute social media offences.[130]

In 2013 Caroline Criado-Perez, an active feminist campaigner publicly spoke out about having the author Jane Austin printed on banknotes in England and Wales. Following this public campaign, she was subjected to horrific abuse on social media. Comments ranged from 'shut up' to 'rape her nice ass.'[131] One individual, Peter Nunn, subjected Ms Criado-Perez to a crusade of abuse:

> 'He dug up my work history. He dug up my relationship and family history. He dug up my family's work history - including publishing home addresses. He wrote reams of blogs about me and my every public move. He made numerous videos about me. He set up numerous [T]witter accounts all of which spoke almost exclusively about me. In these same [T]witter accounts he detailed the best way to rape and drown a witch, alongside repeatedly naming me as the head of the "witches' coven". He also boasted on [T]witter in the same account about having bought a gun, and wondered "how much death" this gun could buy him.'[132]

---

[128] Facebook, 'Create An Account' (*Facebook*, 2017) <https://www.facebook.com/help/345121355559712> accessed 12 November 2017

[129] Azy Barak, 'Sexual Harassment on the Internet' (2005) 23(1) Social Science Computer Review 77

[130] May Bulman, 'Victim of online harassment feels "absolutely hopeless" over police inaction' *The Telegraph* (London, 6 July 2017) <http://www.independent.co.uk/news/uk/home-news/online-harassment-victim-sussex-police-inaction-absolutely-hopeless-a7825691.html> accessed 12 November 2017

[131] Alexandra Topping, 'Jane Austen Twitter row: two plead guilty to abusive tweets' *The Guardian* (London, 7 January 2014) <https://www.theguardian.com/society/2014/jan/07/jane-austen-banknote-abusive-tweets-criado-perez> accessed 10 October 2016

[132] Caroline Criado-Perez, 'A Brief Comment on Peter Nunn, Sentenced Today For Twitter Abuse' (*Week Women*, 2014) <https://weekwoman.wordpress.com/2014/09/29/a-brief-comment-on-peter-nunn/> accessed 29 October 2016

Despite a clear course of conduct being present, which arguably amounted to harassment and caused Ms Criado-Perez distress, Nunn was prosecuted and found guilty of sending grossly offensive communications contrary to the Communications Act 2003, receiving a six week custodial sentence.[133] Subsequently, the police are failing to adequately apply the Protection from Harassment Act in relation to social media offences, as highlighted further in the prosecution statistics.

Each year the CPS conducts a report specifically scrutinising violence against women and girls in England and Wales. The 2016 to 2017 report exposed that the number of prosecutions brought under the Protection from Harassment Act, declined between 2016 and 2017 by 8.4%.[134] As a result, an investigation was conducted by the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate in July 2017. The investigation looked into how the police and the CPS use the Protection from Harassment Act to prosecute the conduct of harassment and stalking offences across England and Wales.

The report exposed a complete failure by the police to investigate, report and put forward cases to the CPS for possible prosecution under the Protection

[133] *R v Peter Nunn* The City of London Magistrates Court 29 September 2014 (unreported)
[134] The Crown Prosecution Service, 'Violence against women and girls report: tenth edition' (*CPS.gov*, 2017) 7 <https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2017.pdf> accessed 19 February 2017. Please note, there is an issue with these statistics. As uncovered by the Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate, police forces and the CPS have confused the definitions of stalking and harassment. Consequently, it can be argued that these figures do not truly represent the extent of harassment and stalking.

from Harassment Act, especially where social media related offences were concerned. Instead victims were advised to withdraw from social media:

> '"It wasn't her (the perpetrator's) fault for sending abusive Facebook messages, it was my fault for being on Facebook … And the only way to stop these messages is if I deactivate [*sic*] my Facebook account, and come off social media."'[135]

As discussed in chapter one, this approach by the police in relation to social media abuse is similar to rape myth assumptions made and given to women in order to 'reduce' the likelihood of sexual assault. The term rape 'myth assumption' was first introduced in the 1970s and is used to describe 'a complex set of cultural beliefs thought to support and perpetuate male sexual violence against women.'[136] For instance, telling women 'not to walk home alone in the dark' or 'not to wear revealing clothing' if they do not wish to be raped. These assumptions presumed if women refrain from partaking in these types of behaviours, it would reduce their risk of being assaulted. This approach is now being mirrored in relation to online abuse. Individuals who are being subjected to abuse online are being advised by the authorities to remove their online presence, with a stigma still being attached within the police when it comes to social media related abuse.[137] From a victimology stance, here the complainant is being judged on their own victimisation for

---

[135] Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate n.102, 52

[136] Diana L. Payne, Kimberly A. Lonsway, & Louise F. Fitzgerald, 'Rape myth acceptance: Exploration of its structure and its measurement using the Illinois Rape Myth Acceptance Scale' (1999) 33 Journal of Research in Personality 27

[137] College of Policing, National Crime Agency and National Police Chief's Council, 'Digital Investigation and Intelligence: Policing capabilities for a digital age April 2015' (*NPCC*, April 2015) <http://www.npcc.police.uk/documents/reports/Digital%20Investigation%20and%20Intelligence%20Policing%20capabilities%20for%20a%20digital%20age%20April%202015.pdf> accessed 4 January 2018. See also, David Barrett, 'Police "dismissive" of online crime, finds watchdog' *The Telegraph* (London, 22 December 2015) <http://www.telegraph.co.uk/news/uknews/crime/12064353/Police-dismissive-of-online-crime-finds-watchdog.html> accessed 4 January 2018

simply having a social media account. By taking this approach to online abuse we are not apricating the emotional turmoil associated with becoming a target of online abuse, or indeed, placing the victim at the centre of the criminal justice system.

Stalking

As previously stated, before 2012 stalking and harassment were treated as the same offence, and both governed under section 1 of the Protection from Harassment Act. In 2012 the conduct of stalking was specifically implemented into the Protection from Harassment Act under section 111(1) of the Protection from Freedoms Act 2012, following concerns that the Protection from Harassment Act did not cover stalking sufficiently.[138] Like that of harassment, it has been accepted that this behaviour can occur online and has been coined 'cyberstalking.' Cyberstalking is the continued behaviour of harassing another individual where there is a course of conduct present, *via* the use of the Internet or electronic communications.[139] Though there are issues as to when certain behaviours go from cyber harassment to cyberstalking.

MacEwan states that not only has the Internet introduced new stalking behaviours, but it also allows for direct contact between the perpetrator of the offence and the victim, which in many cases can occur 'around the clock'.[140]

[138] Neil MacEwan, 'The new stalking offences in English law: will they provide effective protection from cyberstalking?' (2012) 10 Criminal Law Review 767
[139] Paul Bocij, *Cyberstalking: Harassment in the Internet Age and how to Protect Your Family* (Praeger Publishers 2004) 3-4
[140] MacEwan n.138, 771

In July 2016 Chloe Cowan[141] was sentenced to 3 years imprisonment for cyberstalking offences under the Protection from Harassment Act for sending 'vile' tweets online.[142] Cowan set up several fake Twitter accounts to stalk Denise Fergus, the mother of James Bulger (a toddler who was murdered in 1993) to taunt her about her son's death. Messages were sent directly to Ms Fergus' social media account and resulted in her fearing to leave her own home.

Despite arguments being raised in 2012 that cyberstalking should be specifically included in the Protection from Harassment Act, it was considered unnecessary,[143] as explained further in later parts of this discussion. Therefore, section 2A of the Protection from Harassment Act is used to prosecute cyberstalking offences today. This section of the Protection from Harassment Act takes a very similar format to that of section 1 of the Act.[144] The *actus reus* consists of a course of conduct, which fulfils the requirements for harassment. Like that of section 1, a course of conduct is considered contact that occurs on at least two occasions, which would alarm a person or cause them distress to satisfy the element of harassment where one person is committing the offence.

---

[141] *R v Chloe Cowan* Canterbury Crown Court 14 July 2016 (unreported)
[142] ITV News, 'Student who sent "vile" tweets to murdered James Bulger's mother jailed for three years' *ITV News* (London, 14 July 2016) <http://www.itv.com/news/2016-07-14/student-who-sent-vile-tweets-to-murdered-james-bulgers-mother-jailed-for-three-years/> accessed 20 October 2016
[143] Home Office, *'The Protection from Harassment Act 1997: Improving Protection for Victims of Stalking'* (2012) 17
[144] Under section 4A of the Protection from Harassment Act 1997 a further offence is included- stalking involving fear of violence or serious alarm or distress. If it can be found that the person being stalked was in fear of violence or serious alarm or distress, this section of the Act should be used to prosecute the defendant.

In addition to this, it must be found that the behaviour being complained about amounts to stalking. As previously mentioned, there is no definition of stalking contained in the Act, instead a non-exhaustive list of behaviours is included:

> '… (a) following a person; (b) contacting, or attempting to contact, a person by any means; (c) publishing any statement or other material – (i) relating or purporting to relate to a person, or (ii) purporting to originate from a person; (d) monitoring the use by a person of the internet, email or any other form of electronic communication; (e) loitering in any place (whether public or private); (f) interfering with any property in the possession of a person; [and] (g) watching or spying on a person'.[145]

If the conduct being complained about can be regarded as stalking and a course of conduct is present which amounts to harassment, then the *actus reus* for section 2A of the Protection from Harassment Act will be satisfied.[146] In addition, similar to that of section 1(1)(b), the *mens rea* for the offence of stalking is based on the construction of knowledge. Here, it must be found that the perpetrator 'knows or ought to know that the[ir] behaviour would amount to [the] harassment of another.'[147]

As previously mentioned during the consultation period before the insertion of section 2A into the Protection from Harassment Act, concerns were raised that the Act should specifically criminalise cyberstalking, but this was dismissed:

---

[145] Protection from Harassment Act 1997 2A(3)

[146] It is important to note that under section 4A(4) of the Protection from Harassment Act, there is a defence available with regard to a course of conduct that amounts to stalking: '… (a) A's course of conduct was pursued for the purpose of preventing or detecting crime or, (b) A's course of conduct was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under any enactment, or (c) the pursuit of A's course of conduct was reasonable for the protection of A or another or for the protection of A's or another's property.'

[147] Protection from Harassment Act 1997 2A 2(c)

> ‘A number of respondents raised concerns relating to cyberstalking. For the most part, social network site operators adopt sensible and responsible positions on illegal, inappropriate and offensive content hosted on their sites in the terms and conditions they require for use of their services. Internet service providers and social media also already have a legal obligation to cooperate with the police during investigations of allegations of harassment and stalking.’[148]

However, the concept that social media companies are under a legal obligation to cooperate with the police has now been overruled by the Court of Justice of the European Union in the joined cases of *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others.*[149] The Court of Justice of the European Union was asked to rule on the legality of the Conservative Governments approach to surveillance of communications, in relation to combatting terrorism in the United Kingdom.

Under the Investigatory Powers Act 2016 the Government attempted to force website hosts and phone companies to hold citizens communication data for twelve months, allowing the police and other government agencies access to this information.[150] It was ruled by the Court of Justice of the European Union that only in cases relating to terrorism, could the Government force companies to hand over data. Consequently, social media companies are not under a legal obligation to work with the police in matters of online abuse.

---

[148] Home Office n.143, 17

[149] C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* [2016] ECLI 970

[150] Alan Travis, ‘“Snooper's charter” bill becomes law, extending UK state surveillance’ *The Guardian* (London, 29 November 2016) <https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance> accessed 8 January 2018

For instance, Twitter has been criticised for its reluctance to disclose information to legal authorities when approached.[151]

In 2017 the UK Home Affairs Committee held a review examining hate crime and extremist content, which was being made available on social media sites.[152] Representatives from Facebook, Twitter and YouTube[153] attended the committee meeting to respond to questions posed to them by MPs about their role in reducing abusive and extremist content on their sites. All three companies were criticised for being slow in the removal of such content:

> 'The biggest companies have been repeatedly urged by Governments, police forces, community leaders and the public, to clean up their act, and to respond quickly and proactively to identify and remove illegal content. They have repeatedly failed to do so.'[154]

Social media companies are not only reluctant in working with the criminal justice system to disclose information contained on their sites but also, slow in the application of removing abusive content.[155] With continued issues relating to social media companies being slow in aiding law enforcement, pressure has been placed on the criminal justice system to adequately

---

[151] Christopher Williams, 'Twitter refuses to hand member information to police' *The Telegraph* (London, 29 January 2013) <http://www.telegraph.co.uk/technology/twitter/9834776/Twitter-refuses-to-hand-member-information-to-police.html> accessed 4 January 2018. In May of 2018 Facebook released the scale of abuse on its site, though there are issues with the data given. See, Laura Bliss, 'What Facebook isn't telling us about its fight against online abuse' *The Conversation* (London, 21 May 2018) <https://theconversation.com/what-facebook-isnt-telling-us-about-its-fight-against-online-abuse-96818> accessed 29 May 2018

[152] Home Affairs Committee, *Hate crime: abuse, hate and extremism online* (HC 2016-17, 609)

[153] Only these three social networking companies were present as they are the only companies with representatives in the United Kingdom.

[154] Home Affairs Committee n.152, [36]

[155] The Fawcett Society, 'Twitter is "failing women" experiencing online threats and harassment' (*The Fawcett Society*, 22 August 2017) <https://www.fawcettsociety.org.uk/news/twitter-failing-women-experiencing-online-threats-harassment> accessed 16 February 2018

support victims of online abuse. Yet law enforcement has continued to misunderstand cyberstalking:

> 'Basically they've told me [the police], any contact that I receive through social media is irrelevant, because they can't prove that it's associated to them [the abuser].'[156]

Despite cyberstalking not specifically being included in the Protection from Harassment Act and misunderstandings by the police, there have been some successful prosecutions under the Act for this offence. The first conviction for cyberstalking occurred in 2014,[157] though this was two years after the behaviour of stalking was included in the Act. Furthermore, the conduct of cyberstalking has been researched since the turn of the last millennium. For instance, in 2003 Bocij examined the extent of cyberstalking within society. Using an email snowballing sample, he surveyed 169 participants to examine their understanding of cyberstalking, as discussed in detail in chapter one. Yet it took eleven years before the first conviction for cyberstalking. Arguably, the law has been extremely slow in prosecuting stalking offences conducted online.[158]

The Protection from Harassment Act: An Overview

[156] Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate n.102, 27
[157] *R v Andrew Meldrum* Woolwich Crown Court 30 May 2014 (unreported). See also, Nicola Fifield, 'Cyber stalker bugged women's computers to spy on them in their bedrooms' *The Telegraph* (London, 30 May 2014) <http://www.telegraph.co.uk/news/uknews/crime/10866262/Cyber-stalker-bugged-womens-computers-to-spy-on-them-in-their-bedrooms.html> accessed 25 October 2016
[158] For another study looking at the effects of cyberstalking see, Antony Brown, Carsten Maple & Emma Short, 'Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey' (*University of Bedfordshire National Centre for Cyberstalking Research*, 2011) <https://www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf> accessed 25 October 2016. See chapter one for more information on this study.

The overall use of the Protection from Harassment Act to govern both cyber harassment and cyberstalking is flawed. Recently, the police and the criminal justice system have come under criticism with the way in which they deal with complaints of harassment and stalking, both in the physical world and online.[159] This was exposed in detail in the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate report into the Protection from Harassment Act in July 2017. The report exposed a complete failure in the justice system to take the behaviours of harassment and stalking seriously, particularly where social media was facilitated in the offence.[160] The report goes further to find a failure by some police forces to link all conduct undertaken by a defendant together, despite the social media prosecution guidelines emphasising the importance of this:

> 'Where an individual receives unwanted communications from another person *via* social media in addition to other unwanted behaviour, all the behaviour should be considered together in the round by the prosecutor when determining whether or not a course of conduct is made out.'[161]

The guidelines make numerous remarks reminding prosecutors to consider the Protection from Harassment Act, yet there has been a decline in prosecutions under this Act of Parliament.

In addition, the report found a lack of understanding between forces as to what constitutes harassment or stalking, specifically the difference between the two behaviours under the Protection from Harassment Act. From a study

[159] Rachel Horman, 'We have a stalking law – so why don't the police use it?' *The Guardian* (London, 19 August 2016) <https://www.theguardian.com/commentisfree/2016/apr/19/stalking-law-police-lily-allen-stalked-criminal-justice-system> accessed 22 November 2017
[160] Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate n.102, 52
[161] The Crown Prosecution Service n.47

of 112[162] police reports across six forces it was found that the police had failed to deal with any of these cases correctly and in many matters, misunderstanding the severity of the behaviour being reported. Salter and Bryden suggest that the Protection from Harassment Act is 'the most powerful shield available to an online user', yet there is a failure by the criminal justice system to use the Act correctly to protect social media users from online abuse. [163]

It has been accepted that the Protection from Harassment Act can govern online behaviour, and this has been somewhat successful. Nonetheless, the review conducted of the Act in 2017 uncovered misunderstandings between the behaviours of stalking and harassment within the criminal justice system:[164]

> '… [L]egislation does not exhaustively define stalking or the particular circumstances that make stalking different from those of harassment. Therefore, without any additional clarification, what differentiates harassment and stalking can be open to interpretation and result in confusion.'[165]

Consequently, a recommendation has been put forward in the report for a more definitive definition of stalking to try and combat this issue. Nevertheless, the current lack of clarity in the Protection from Harassment Act is another example of a fundamental breach of legality, especially where social media is facilitated to commit the offence. In addition, as highlighted

[162] Of these 112 case studies, 82 had elements of social media/technology-based offences.
[163] Salter & Bryden m.123, 100
[164] This was further affirmed by the Law Commission. See, Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018) [8.161]
[165] Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate n.102, 24

above the Protection from Harassment Act is currently being underutilised in social media prosecutions.

As previously stated, in the case of *Nunn,* one of the individuals convicted for sending abusive tweets to the feminist campaigner Caroline Criado-Perez, his actions could have constituted a clear breach of the Protection from Harassment Act, yet he was convicted under section 127(1) of the Communications Act 2003 for the sending of grossly offensive comments. This further suggests that the law is currently not being used to its full capacity, leaving victims frustrated at the criminal justice system.[166]

Chapter Overview

The extent of online abuse today means in certain cases the criminal law needs to intervene. This chapter has examined three non-technology-based Acts of Parliament, the Serious Crime Act 2007, the Public Order Act 1986 and the Protection from Harassment Act 1997, which have all been adapted to fit a technology-based age. There are however flaws in their application in governing social media related offences in particular, online abuse.

The intention of the Serious Crime Act was to criminalise organised and serious crime within society. Yet the Act has since been used to prosecute individuals for the creation of Facebook event pages during the 2011 riots in the United Kingdom, which can be suggested as being beyond the scope of Parliament's original intentions. Legality in the criminal law, as crystallised by

[166] Caroline Criado-Perez n.132

Luban[167] and Fuller[168] means that legal provisions need to be action-guiding. Here, citizens behaviour should be governed in the context of clear and distinct rules. The Serious Crime Act and its use in *Blackshaw*[169] and *Sutcliffe-Keenan*,[170] can be considered as a breach of the action-guiding principle of the criminal law. As discussed previously, the provisions contained in sections 44 to 46 of the Act lacks clarity, and consequently individuals cannot govern their behaviour in accordance with the law. Virgo has gone as far as to state that the Serious Crime Act 'needs to be put out of its misery and we need to start again.'[171]

Similarly, the Public Order Act lacks certainty in its application to offences carried out with the aid of social media. For Dorfman the use of the Public Order Act in the matter of *Stacey*[172] was a clear abuse of the law.[173] The purpose of the Public Order Act was to prosecute offences which incited racial hatred, an element which Dorfman considers to be missing in *Stacey*. Furthermore, the law lacks certainty as to when the Public Order Act should be utilised when it comes to social media abuse. As discussed above the Act was used to prosecute Stacey for the sending of racist tweets, but it was not used in relation to *Chabloz* [174] who published videos of an anti-Semitic nature. More recently, the Public Order Act has been used to arrest

[167] David Luban, 'Fairness to rightness: Jurisdiction, Legality, and the Legitimacy of International Criminal Law' in Samantha Besson & John Tasioulas (eds), *The Philosophy of International Law* (Oxford University Press 2010) 37
[168] Lon L Fuller, *The morality of law* (Yale University Press 1964)
[169] *Blackshaw* n.28
[170] *Perry Sutcliffe-Keenan* n.30
[171] Virgo n.21
[172] *Liam Stacey* n.71
[173] Dorfman n.74
[174] *Alison Chabloz* n.84

individuals for the publication of a video on social media, in which they burnt a replica of Grenfell Tower.[175] Yet there continues to be issues with the principle of legality and the use of the Public Order Act in a social media setting.

Whereas the use of the Serious Crime Act and the Public Order Act can be considered as an abuse of the law, the Protection from Harassment Act is being underutilised in the criminal justice system, particularly when examining cyber harassment and cyberstalking. The lack of clarity contained within key provisions of the Act means at times mistakes are being made in the criminal justice system. This is further confirmed by the Law Commission who argue that a lack of a distinct definition between harassment and stalking puts victims at a disadvantage. As put by the Law Commission:

> '[r]esearch suggests that the prevalence of online harassment is high, and stalking by a person unknown to the victim is more common online than offline.'[176]

Chapter Four: Recommendations

- Create a clear and precise legal rule regulating the encouragement of another to commit a further criminal offence or incite others to target another online;

[175] Grenfell Tower was a block of flats in London which caught fire in 2017, killing 72 people. See, Adam Withnall, 'Grenfell Tower bonfire effigy burning leads to five arrests' *The Independent* (London, 12 February 2019) <https://www.independent.co.uk/news/uk/crime/grenfell-tower-bonfire-effigy-video-fire-burning-guy-fawkes-november-5-a8619491.html> accessed 12 February 2019. In April 2019, it was announced that one individual had been charged contrary to section 127(1) of the Communications Act 2003. He was later found not guilty.
[176] Law Commission n.164, [8.9]

- Ensure the social media prosecuting guidelines are updated to include examples to illustrate when a comment or conduct breaches legal provisions;
- Create a clear and precise legal rule regulating online hate speech. Here, what constitutes hate speech will be expanded to cover a range of protected characteristics, including gender;
- With the aid of section 4A of the Public Order Act 1986 create a legal provision that conforms to the principle of legality specifically criminalising cyber harassment and cyberstalking;
- Better training for police forces as to what constitutes harassment and stalking, especially those conducted online; and
- A clearer definition as to what constitutes cyber harassment and cyberstalking.

Chapter Five

Social Media, Criminal Law Regulation and Technology-Based Legislation: Part One

> '"Twitter is not just a closed coffee shop among friends. It goes out to hundreds of thousands of people and you must take responsibility for it. It is not a place where you can gossip and say things with impunity, and we are about to demonstrate that."'[1]

In England and Wales there is currently no specific Act of Parliament aimed at criminalising inappropriate behaviour on social media sites. Instead, as explored in the previous chapter the criminal justice system has had to adapt legislation to fit a social media context. Despite this there are several legal provisions which have been created from a technological perspective, including, but not limited to, the Computer Misuse Act 1990, section 33 of the Criminal Justice and Courts Act, the Malicious Communications Act 1988 and section 127 of the Communications Act 2003.

Though all the above govern technology-based offences, with the exception of section 33 of the Criminal Justice and Courts Act, these legal provisions were not necessarily created with social media in mind. In fact, the Computer Misuse Act, the Malicious Communications Act and the Communications Act all predate Facebook and Twitter, two of the biggest social media companies today. Yet like that of the Serious Crime Act 2007, the Public Order Act 1986 and the Protection from Harassment Act 1997, as discussed in chapter four, the Computer Misuse Act, the Malicious Communications Act, and section

[1] Andrew Read (Solicitor) found in Laura Scaife, 'The DPP and social media: a new approach coming out of the Woods?' (2013) (18)1 Communications Law 5, 9

127 of the Communications Act have since been used to prosecute social media-based offences.

This chapter will discuss the current use of the Computer Misuse Act and section 33 of the Criminal Justice and Courts Act in governing inappropriate behaviour online. The Malicious Communications Act and section 127 of the Communications Act will be examined separately in the following chapter because, of the technology-based legislation, it is the latter two that have given rise to most social media criminality.

Computer Misuse Act 1990

The Computer Misuse Act was enacted into the legal system of England and Wales to help tackle the growing issue of computer misuse, which was affecting businesses worldwide, in particular computer hacking. Though it is rare the Computer Misuse Act has been used to prosecute defendants who have 'hacked' social media profiles to torment another.[2] The discussion below will outline the background behind the Acts implementation, before examining both the *actus reus* and *mens rea* of sections 1 to 3 of the Computer Misuse Act.

During the 1900s technology started to evolve within society, with computer usage increasing throughout the 1960s.[3] Though there is no true definition of 'computer', the courts have come to define it as a '… device for storing,

[2] Laura Scaife, *Handbook of Social Media and the Law* (Routledge 2015) 183
[3] Stefan Fafinski, *Computer Misuse* (Routledge 2009) Chapter Three

processing and retrieving information.'[4] As technology expanded new criminal acts started to occur across the globe, commonly referred to as computer misuse. Computer misuse involves '… offences or attacks against computer systems such as hacking or denial of service (DOS) attacks.'[5] Prior to the Computer Misuse Act, other Acts of Parliament were being used to criminalise computer misuse in the 1970s and 1980s. Nevertheless, issues arose with the adaption of these Acts of Parliament, which were never intended to cover technology-based crimes.

In *Cox v Riley*[6] the court had to decide whether the actions of the defendant in erasing data from a printed circuit card, amounted to criminal damage under the Criminal Damage Act 1971. By applying the *actus reus* of the Criminal Damage Act, the damage of property belonging to another, contained in section 1 of the Act, it was held that the defendant had committed an offence under this Act of Parliament.

Though the criminal justice system was able to pursue a successful prosecution in *Cox*, the use of the Criminal Damage Act to prosecute computer misuse offences did create some problems within the legal system. The conduct of criminal damage is an offence which is triable either way, meaning that the case can be brought before the Magistrates Court or the Crown Court depending on the value of the damage, as defined under

[4] *Director of Public Prosecutions v McKeown* [1997] 1 W.L.R. 295 per Lord Hoffman 302
[5] The Crown Prosecution Service, 'Computer Misuse Act 1990' (*CPS.gov*, 2018) <https://www.cps.gov.uk/legal-guidance/computer-misuse-act-1990> accessed 23 January 2018
[6] *Cox v Riley* (1986) 83 Cr. App. R. 54

section 22 of the Magistrates' Courts Act 1980. Until 1994, if the damage to property exceeded more than £2,000 the case would be held before the Crown Court.[7] In traditional cases of criminal damage this would be easy for the courts to distinguish. However, in cases relating to technology it was not always easy to value the cost of the damage which had occurred.[8]

Furthermore, not all cases of computer misuse resulted in successful prosecutions. In the 1980s two individuals hacked into British Telecom's (BT) systems gaining access to private information stored on BT's private network.[9] They were originally prosecuted under the Forgery and Counterfeiting Act 1981, later being overturned by the Court of Appeal. The judgment of the Court of Appeal was upheld by the House of Lords:

> 'The appellants' conduct amounted in essence, as already stated, to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts.'[10]

Essentially, it was held by the Law Lords that there was no criminal offence under English Law that amounted to computer hacking; the defendants were cleared of all charges. Following high profile media cases such as *Gold*, concerns were raised about 'the misuse of computers or computer systems' across the globe.[11]

[7] The value is now £5,000 as amended by the Criminal Justice and Public Order Act 1994 section 46.
[8] Law Commission, *Criminal Law: Computer Misuse* (Law Com No 1986, 1989) [2.32]
[9] *R v Gold (Steven William), Schifreen (Robert Jonathan)* [1988] A.C. 1063
[10] *Ibid.,* per Lord Justice Lane 1124
[11] Law Commission n.8, [1.1]

In 1989 the Law Commission conducted a report examining the issues of computer misuse following:

> '[a]n increasing degree of interest and disquiet [becoming] apparent in recent years in relation to the implications of, and the possible misuse of, the computerisation that plays an ever growing role in public, commercial and indeed in private life.'[12]

The report focused on the public need to criminalise computer misuse, paying particular reference to how this conduct impacted on commercial businesses:

> 'Accordingly, after the consultation had closed in March 1989 we arranged a series of meetings with computer and software manufacturers, computer users in commerce, industry and the banking and financial sectors, and those responsible for seeking to apply the existing criminal law to cases of computer misuse, in order to seek a better understanding of the problems that had evoked the expression of opinion on consultation …'.[13]

The Law Commission examined in detail the legislative framework already enacted which could be used to prosecute offences of computer misuse. They concluded that there was a gap in the law which needed to be filled to fully criminalise this behaviour, due to the high costs that were experienced by companies who became subject to this type of conduct. As a result, the recommendations within the report were aimed at protecting businesses from three growing areas of computer misuse: computer fraud, hacking and the alteration of computer data or functions.

Computer fraud was considered by the Law Commission as the manipulation of a computer network to dishonestly '… obtain money, property or some other advantage of value or to cause loss',[14] which was becoming a growing

[12] *Ibid.,* [1.1]
[13] *Ibid.,* [1.10]
[14] *Ibid.,* [2.2]

problem in the 1970s and 1980s.[15] In the consultation period before the Law Commission's report into computer misuse was completed, many companies spoke of their losses due to computer fraud. For example, one company suffered substantial losses after a computer was reprogramed to produce bogus cheques and false entries into a banking system.[16]

Though the law already criminalised fraudulent behaviour under the Forgery and Counterfeiting Act, it was not always successfully used in cases of computer fraud, as illustrated in *Gold*. Under section 1 of the Forgery and Counterfeiting Act:

> '[a] person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it to do or not to do some act to his own or any other person's prejudice.'

The term instrument under the Act is defined as '… any disc, tape, sound track or other device on or in which information is recorded or stored by mechanical, electronic or other means.'[17] Here, there must be a stored record of the omission. In *Gold* the computer software had wiped the defendant's credentials meaning there was no record of their actions, the rationale behind the case being dismissed.

One of the major foundations for the Law Commission's investigation into computer misuse surrounded the conduct of hacking. Computer hacking is:

> '… the modification of technology, such as the alteration of computer hardware or software, in order to allow it to be used in innovative

[15] Andrew D Chambers, 'Computer fraud and abuse' (1977) 21(3) The Computer Journal 194
[16] Law Commission n.8, [2.4]
[17] Forgery and Counterfeiting Act 1981 section 8(1)d

ways, whether for legitimate or illegitimate purposes.'[18]

Concerns were raised about hacking following the growing need to protect confidential and private information, as the use of computers increased throughout the United Kingdom and the globe:

> 'Two French hackers, for example, broke into a life-support system in a hospital's intensive care unit and, perhaps unwittingly, turned it off. There are several known instances of people breaking into air traffic control systems. One trembles to think of the dangers of that ...'.[19]

Examples of computer hacking, similar to those given above, were specified to illustrate the importance of criminalising this conduct, as the legal framework prior to the enactment of the Computer Misuse Act was inadequate in prosecuting computer hackers. Between 1985 and 1990, 270 cases of computer misuse, many relating to hacking, had been confirmed by the Department of Trade and Industry. Of these cases only six were brought before the courts, of which three cases resulted in successful prosecutions.[20]

The final conduct which the Law Commission investigated was the use of technology to alter or destroy information held on a computer, concluding that there were several ways in which this conduct could be carried out, for instance the 'physical destruction, electronic erasure [and through] viruses and worms.'[21] Emphasis was placed on the substantial losses that can be experienced by businesses who were subjected to this form of computer misuse, whilst also finding that the legal framework in the 1980s did not adequately criminalise this conduct. Therefore, the Law Commission

[18] Thomas J. Holt, Adam M. Bossler & Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2nd edn, Routledge 2017) Chapter three
[19] HC Deb 9 February 1990, vol 166, cols 1161-1162
[20] HC Deb 9 February 1990, vol 166, col 1134
[21] Law Commission n.8, [2.26]

suggested a change in the law, putting forward draft recommendations as to what should be included in an Act criminalising computer misuse.

Throughout the Law Commission's report an emphasis was placed on protecting corporations from the ever-growing mischief of computer misuse. References were made to public sector companies such as the NHS and air traffic control systems, but most of the report focused on private companies who had become subjected to computer misuse. Therefore, the recommendations made by the Law Commission focussed on the protection of large corporations, rather than separate individuals, an element reflected within the Computer Misuse Act itself. Following the numerous cases of computer misuse and the report conducted by the Law Commission, a Private Members' Bill was introduced into Parliament in 1990 by Michael Calvin MP, which later received Royal Assent to become the Computer Misuse Act.[22]

The Computer Misuse Act governs, 'unauthorised access to computer material',[23] 'unauthorised access with intent to commit or facilitate commission of further offences',[24] and 'unauthorised acts with intent to impair, or with recklessness as to impairing, [the] operation of [a] computer, ect'.[25] Section 1 of the Act makes it an offence for an individual to attempt to secure access to any data or programme held on another person's

[22] Private Members' Bill are introduced into Parliament by MPs who are not Government Ministers. For more information on how this procedure works see, Mark Elliot & Robert Thomas, *Public Law* (3rd edn, Oxford University Press 2017) 219
[23] Computer Misuse Act section 1
[24] Computer Misuse Act section 2
[25] Computer Misuse Act section 3

computer. The *actus reus* of the offence is in the unauthorised attempt to access data or a programme held on another's computer. Here, the term unauthorised has been defined by Parliament in section 17(5) of the Act:

> 'He is not himself entitled to control access of the kind in question to the program or data; and he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.'

The Crown Prosecution Service (CPS) guidelines on the Computer Misuse Act states that there does not have to be a specific attempt to access a certain programme or data held on the computer.[26] Whereas the *mens rea* of the offence consists of two elements: knowledge and intent. Here, the defendant must have the knowledge that their intended actions of accessing the information are unauthorised, mere recklessness will not suffice.[27]

The defendant does not need to physically access the information, he merely needs to attempt to do so in order to be liable under section 1 of the Computer Misuse Act, though there needs to be an awareness that by doing so they are committing an unauthorised act.[28] In a social media context this would be the actions of hacking into another person's social media profile. There is no need to cause a person alarm or distress. Put simply, the actions of accessing another individual's social media account without prior authorisation would amount to a breach of section 1 of the Computer Misuse Act.

[26] The Crown Prosecution Service n.5
[27] *Ibid.,*
[28] Computer Misuse Act section 1(1)c

This is demonstrated in *R v Gareth Crosskey*.[29] Crosskey hacked into the social media account of the famous actress Selena Gomez by deceiving Facebook staff. Among other things, this gave him access to her personal emails. Using this information, he published several statements online, including a comment allegedly taken from Ms Gomez's account stating that 'Justin Bieber sucks'.[30] Following this message being made publicly available, Ms Gomez received abusive and threating messages *via* social media. In addition, Crosskey attempted to sell the personal information he had gained from the unauthorised access to other media outlets, including high profile newspaper tabloids. He was subsequently charged and convicted under section 1 and section 3 of the Computer Misuse Act.[31]

Though as previously mentioned, under the Computer Misuse Act there is no requirement to cause an individual distress or alarm, it was an aggravating factor which the court took into consideration when sentencing Crosskey:

> '… there was the element of harm to Mr Teefey [her father] and to Miss Gomez. The claim that he had access to four of her personal e-mail accounts caused distress and the fear of wide dissemination of personal and intimate correspondence with Mr Bieber on the web. As we have already observed, following the unauthorised access to the account, there was the posting 'Justin Bieber sucks'. That could not be attributed to the appellant, but it had the consequence that fans of Mr Bieber reacted in a manner hostile to Miss Gomez adding to her further distress.'[32]

[29] *R v Crosskey* [2012] EWCA Crim 1645, [2013] 1 Cr. App. R. (S.) 76
[30] It was never proven that Crosskey placed this comment online.
[31] How section 3 of the Computer Misuse Act is applied in a social media context will be explored in later parts of this discussion.
[32] *Crosskey* n.29, per Mr Justice Owen [14]

Crosskey was sentenced to eight months imprisonment for his actions.[33] The investigation into the hacking of Ms Gomez's social media account cost the state £50,000 and was described by the ex-Chief Crown Prosecutor for London as '… the most extensive and flagrant incidence of social media hacking to be brought before [the] British courts.'[34]

The successful prosecution of Crosskey for a breach of section 1 of the Computer Misuse Act can be seen as an appropriate decision by the CPS and the courts. By applying the principle of legality as outlined in chapter two, the Computer Misuse Act can be regarded as accessible and foreseeable. Section 1 of the Computer Misuse Act clearly outlines the offence:

> 'A person is guilty of an offence if he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured; the access he intends to secure, or to enable to be secured, is unauthorised; and he knows at the time when he causes the computer to perform the function that that is the case.'[35]

It is therefore foreseeable to the public that if they were to access another computer without authorised permission, they will have committed an offence under this section of the Act. With reference to Crosskey he would have known that his actions would have been unlawful, and he was consequently prosecuted under the correct Act of Parliament.

[33] At Southwark Crown Court Crosskey was sentenced to 12 months imprisonment. On appeal this was reduced to 8 months.
[34] Alison Saunders, 'Facebook Hacker committed serious offence' (*CPS: News Brief*, 17 February 2017) <http://blog.cps.gov.uk/2012/02/facebook-hacker-committed-serious-offence.html> accessed 11 October 2017
[35] Computer Misuse Act section 1

Section 2 of the Computer Misuse Act regulates unauthorised access to a computer system where the defendant had the intention of causing a further illegal act governed by law. This section consists of two elements. First, the defendant must attempt to commit the offence of gaining access to another person's computer without permission, as governed under section 1 of the Act. Second, they must do this in order to commit a further criminal offence which is prescribed by law. For instance, hacking an individual's social media account to gain access to personal information to commit a further fraudulent act, would breach section 2 of the Computer Misuse Act, as fraud is criminalised under the Fraud Act 2006. Though currently there are no social media abuse cases which have used this section of the Computer Misuse Act to prosecute an individual, it remains an important aspect of the law which should be considered when it comes to online abuse.

In a BBC Panorama documentary, it was found that Facebook 'knows more about us than any other government organisation.'[36] With this in mind, it might well be that section 2 of the Computer Misuse Act could become a prevalent part of the criminal law when it comes to governing online behaviour in certain circumstances. For example, if an individual hacked into another person's social media account, obtaining information which is later used to blackmail another, this would amount to a breach of section 2 of the Computer Misuse Act.

[36] BBC Panorama, 'What Facebook Knows About You' (*BBC IPlayer*, 8 May 2017) <https://www.bbc.co.uk/iplayer/episode/b08qgbc3/panorama-what-facebook-knows-about-you> accessed 12 October 2017

The Computer Misuse Act also regulates 'unauthorised acts with intent to impair, or with recklessness as to impairing, [the] operation of computer, etc' under section 3 of the Act. Essentially, this section governs the conduct of damaging another's computer so that it cannot be used, whilst also prohibiting denial of services.[37] Denial of services:

> '… are launched against computer systems or networks to cause a loss of service to users, typically the loss of network connectivity by consuming the bandwidth of the victim network or by overloading its computational resources.'[38]

The *actus reus* of the offence under section 3 of the Computer Misuse Act is the unauthorised access to another's computer system to affect the use of the computer, hinder access to data or programmes or alter data or programmes contained on the device. The *mens rea* covers both intention and recklessness. Section 3 of the Computer Misuse Act was used as a further provision to criminalise the conduct of Crosskey, as mentioned above. After gaining access to Ms Gomez's Facebook profile he subsequently changed her password, denying her and her manager access to the account. Consequently, he was prosecuted for a breach of section 3 of the Computer Misuse Act, along with breaching section 1 of the Act.

Section 3 of the Computer Misuse Act can apply in relation to social media abuse. But like that of the other two sections, its application only occurs in limited circumstances. For instance, hacking another's social media account to taunt and abuse a person. This does not necessarily mean that online abusers do not use the conduct of hacking to target other individuals, it could

[37] This was amended by the Police and Justice Act 2006 section 36
[38] Neil MacEwan, 'The Computer Misuse Act 1990: lessons from its past and predications for its future' (2008) 12 Criminal Law Review 955, 960

be that hacking is underreported due to the disclosure of private information.[39]

Despite the Law Commission emphasising the need to specifically criminalise the conduct of computer misuse there were opposing opinions following the Computer Misuse Act receiving Royal Assent:

> 'When the Computer Misuse Act arrived, some had already questioned why the unauthorised access of confidential information held on a computer should be an offence where if the same information were held on card index no offence would be committed.'[40]

MacEwan suggests that computer hacking is similar to the conduct of trespass to land.[41] At its very basic, trespass is entering another's property or land without seeking permission and is a civil law offence.[42] This is supported further by Brenner, who like that of MacEwan, argues that computer hacking has similar characteristics to that of trespass to land:

> '… hacking is conceptually very similar to trespass in the physical world. Similar to trespass, it involves a violation of a use restriction on property that is committed by someone who has no right to access the property.'[43]

Both Brenner and MacEwan support the concept that computer hacking should be a civil matter due to its similarities with the conduct of trespass. Furthermore, Christie argues that the current criminalisation of computer hacking results in fewer reports to the police for fear of the information

[39] Holt & Schell n.18, 66
[40] MacEwan n.38, 956
[41] *Ibid.,*
[42] Kirsty Horsey & Erika Rackley, *Tort Law* (4th edn, Oxford University Press 2015) 515
[43] Susan W Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Greenwood Publishing Group 2010) 51

making its way into the public domain during criminal court proceedings.[44] Whereas under civil law proceedings the court can balance the competing interests of all parties. For instance:

> '[t]he civil law can endeavour to balance the competing interests in protecting economic endeavour against the desirability of an "open" flow of information in society. The criminal law cannot.'[45]

To bring a case before the civil courts the cost would be inflicted upon the party who has already been subjected to computer misuse. As stated in the Law Commission's report computer misuse can have a financial consequence for the victim.[46] It would be unreasonable to expect individuals to pay further money to take legal action against the perpetrator of the offence. Furthermore, civil law does not necessarily create a strong deterrent for future offenders, unlike that of the criminal law, though as noted in chapter two, deterrence does not necessarily work when it comes to the criminal law.

Despite this, the Law Commission argued that the criminalisation of computer misuse acts as a deterrence factor: 'The deterrence of such invasions of computer systems is a proper public goal.'[47] However, as technology has evolved, prosecutions under the Computer Misuse Act have dropped.[48] Between 1990 and 2013, 339 prosecutions were brought under the Computer Misuse Act, with 262 individuals being found guilty of an

[44] Anna L Christie, 'Should the law of theft extend to information?' (2005) 69(4) Journal of Criminal Law 349, 356
[45] Grant Hammond, 'Theft of Information' (1988) 104(Oct) Law Quarterly Review 527, 528
[46] Law Commission n.8, [1.5]
[47] *Ibid.,* [2.15]
[48] HC Deb 16 May 2012, vol 545, col 175

offence under the Act.[49] Consequently, very few successful prosecutions occur under this Act of Parliament. Whereas pro-criminal law theorists see the Computer Misuse Act as a positive approach to combating computer hacking.

For Wasik the criminal law must intervene with this type of conduct for several reasons.[50] First, computers carry a weight of importance within society. Although Wasik was writing in the early 1990s, this argument is even more relevant today. Most data and personal information is stored online or on a computer network, it is therefore important that this information is protected. Furthermore, as previously indicated social media companies, such as Facebook and Twitter, store vast amounts of information about its users which could be used as a form of online abuse. Second, there is a public interest element to the Computer Misuse Act. Wasik argues that it is in the public interest that individuals do not fear that their computer systems will be hacked.[51] Consequently, it should be seen that society takes the behaviour of hacking seriously. Last, there are national security risks in relation to computer hacking. Though this might not be directly linked to social media abuse, it warrants criminal law intervention therefore providing a prime example as to why the Computer Misuse Act is an important aspect of the criminal law.

[49] Mike Penning, 'Computer Misuse Act 1990: Written question – 222192' (*Parliament.uk*, 22 January 2015) <http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2015-01-27/222192/> accessed 12 October 2017
[50] Martin Wasik, 'Law reform proposals on computer misuse' (1989) Apr Criminal Law Review 257, 260
[51] *Ibid.,*

As discussed above, the Computer Misuse Act has been used in a social media related case, *Crosskey*. Yet the Act is not mentioned in the CPS guidelines on social media offences, a clear oversight by the CPS. Indeed, the Communications Committee in their 2019 report concerning online regulation, support the use of the Computer Misuse Act to target specific online behaviours.[52] The Computer Misuse Act can be considered as an important Act of Parliament in combatting social media abuse. The Act conforms to all principles of legality whether that be from an International Criminal Law perspective or a European approach. For a law to conform to the concept of the rule of law, the legal provision under scrutiny '… must be accessible and so far as possible intelligible, clear and predictable'.[53] The Computer Misuse Act conforms to each of these, intelligibility, clarity and predictability, but its uses are limited when it comes to social media abuse. Essentially the Computer Misuse Act is only applicable where a computer system or programme is hacked by an individual who does not have prior permission to access the information in question. This does not mean however that the Computer Misuse Act is redundant regarding online abuse. There are several scenarios where this Act may be suitable, for example hacking a person's social media account to taunt them with personal information gained from the unauthorised access. For instance, Emily Robins suffered physiological abuse following her ex-boyfriend hacking into her Facebook account.[54] It therefore needs to be referenced in the social media

[52] Communications Committee, *Regulating in a digital world* (HL 2017-19, 299) [11]
[53] Lord Bingham, 'The rule of law' (2007) 66(1) Cambridge Law Review 67, 69
[54] Rosamund Urwin, 'Half of young women on Facebook suffer abuse' *The Sunday Times* (London, 2 March 2018) <https://www.thetimes.co.uk/edition/news/half-of-young-women-on-facebook-suffer-abuse-3lxbhhnjj> accessed 6 March 2019

prosecuting guidelines.

Criminal Justice and Courts Act 2015

Revenge pornography has been described as the ultimate humiliation, with many victims being female.[55] In 2015 the act of disclosing to another a sexual image without the consent of the person in the photo, became a specific criminal offence under section 33 of the Criminal Justice and Courts Act 2015. The following discussion will examine why this conduct was considered so fundamentally wrong, that it was specifically criminalised under an Act of Parliament.

The evolution of technology has not only created new offences which can be conducted online, such as that of online mobbing or doxing, it has also allowed offences which were once conducted in a private setting to emerge in an online context, this is especially true in relation to revenge pornography. Revenge pornography is:

> 'the sharing of private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress.'[56]

Though this conduct can occur offline in a technology-based world revenge porn is a growing online industry. In some cases, specifically designed websites have been created to solely host sexual images for revenge purposes.[57] The first website created as a platform for revenge porn

[55] HC Deb 19 June 2014, vol 582, col 1368
[56] HM Government, 'Revenge Porn: The Facts' (*Gov.uk*, 2014) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/405286/revenge-porn-factsheet.pdf> accessed 19 October 2016
[57] It is currently legal for websites to display revenge pornography, but it is illegal for a person to upload a picture to these websites.

emerged in 2010: ‘isanyoneup.com’. In its first week alone the website had more than 14,000 views and in one three month period received 10,000 photo submissions.[58] It has even been reported that in some instances women have been forced to send naked pictures of themselves to website hosts in order to verify their identity, to get explicit pictures of themselves removed from these sites.[59]

The behaviour of revenge porn can have detrimental effects on a person’s wellbeing and in some cases has resulted in psychological harm, including victims being diagnosed with post-traumatic stress disorder,[60] resulting in a loss of employment,[61] and consequently becoming withdrawn from social life.[62] The behaviour of revenge pornography caught the media’s attention in 2012 following a sexually explicit video of Tulisa Contostavlos, who at the time was a judge on the reality TV show ‘The X Factor’, being posted online by her ex-partner.[63] The video went viral[64] and was reposted across social media sites. Since 2010, the posting of revenge pornography has gone

[58] Scott R Stroud, ‘The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn’ (2014) 29(3) Journal of Mass Media Ethic 168, 170
[59] Alistair Carmichael, ‘Better protection for victims of “revenge porn”’ (*alistaircarmichael*, 2016) <http://www.alistaircarmichael.co.uk/amendments_to_crime_and_policing_bill> accessed 11 December 2017
[60] Samantha Bates, ‘“Stripped”: An Analysis of Revenge Porn Victims’ Lives after Victimization’ (Master of Arts Thesis, Simon Fraser University 2015) 24
[61] Alisdair A. Gillespie, ‘“Trust me, it's only for me”: “revenge porn” and the criminal law’ (2015) 11 Criminal Law Review 866, 873
[62] Mudasir Kamal & William J. Newman, ‘Revenge Pornography: Mental Health Implications and Related Legislation’ (2016) 44(3) American Academy of Psychiatry and the Law 359, 362
[63] Keith Perry, ‘Revenge porn: some of the biggest celebrity victims’ *The Telegraph* (London, 30 September 2014) <http://www.telegraph.co.uk/news/celebritynews/11129357/Revenge-porn-some-of-the-biggest-celebrity-victims.html> accessed 12 February 2018
[64] Viral means ‘content that is shared quickly and widely because of high interest.’ See, Jeremy Harris Lipschultz, *Social Media Communication: Concepts, Practices, Data, Law and Ethics* (2nd edn, Routledge 2018) 355

beyond specially designed websites, to being actively published and shared on social media web pages.[65]

In 2014 California was the first State in the United States of America to criminalise the conduct of intentionally distributing '… an image of the person depicted engaging in specified sexual acts …' to cause serious emotional distress.[66] Around the same time research started to emerge examining how the law in the UK should also make revenge porn a specific criminal offence. For instance, Mitchell argued that following Parliament's intentions to make amendments to the Coroners and Justice Act 2009, this would have provided the Government with the perfect opportunity to prohibit the behaviour of revenge porn.[67]

Mitchell went further to give an example of how she felt the law should be constructed:

> 'A person (D) commits an offence if- D intentionally or recklessly publishes, disseminates and/or distributes by any means an image of a person over the age of eighteen, either moving or still, captured by D or the subject in any format, of the uncovered, or visible through less than fully opaque clothing, body parts of another identifiable person or an image of another identifiable person engaged in a sexual act, where D knows or ought to know that the depicted person does not consent to the distribution of the image.'[68]

---

[65] Shared means actively reposting another person's comments *via* your own social media profile.
[66] California Penal Code 647 (USA). See also, Suzanne Choney, '"Revenge porn" law in California could pave way for rest of nation' *NBC News* (New York, 3 September 2013) <https://www.nbcnews.com/technolog/revenge-porn-law-california-could-pave-way-rest-nation-8C11022538> accessed 12 February 2018
[67] Justine Mitchell, 'Censorship in cyberspace: closing the net on "revenge porn"' (2014) 25(8) Entertainment Law Review 283
[68] *Ibid.,* 288

For Mitchell, the *actus reus* of the offence would be committed when the defendant published or distributed a sexualised image. The *mens rea* would be built on the construction of knowledge, intention and recklessness, essentially, giving the criminal justice system a wide interpretation of this type of conduct. She states that body parts, under the ideal law prohibiting revenge porn would include:

> '[u]nclothed external genitalia, the perineum and anus of a male or female; Buttocks of a male or female; Breasts and nipples of a female; and covered erectile genitalia of a male.'[69]

Whereas:

> '"sexual act[s]" … is not limited to sexual intercourse including genital-genital, oral-genital, anal-genital, oral-anal, whether between persons of the same or opposite sex.'[70]

The approach taken by Mitchell in criminalising revenge pornography reflects the detrimental effects this type of behaviour can have on a person, as exposed further in the work of Bates.

Bates conducted eighteen semi-structured interviews with revenge porn 'survivors', using a snowballing sample.[71] Her study aimed to expose the mental anguish associated with this form of conduct and its effects on everyday life.[72] Each participant in the study was able to speak freely about their experiences of revenge pornography. For instance, one participant

[69] *Ibid.,* 289
[70] *Ibid.,*
[71] By survivors Bates means those who have been subjected to revenge pornography but uses the term 'survivors' as it 'implies a more empowering label rather than giving "victim" labels that imply less agency.' Samantha Bates, 'Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors' (2017) 12(1) Feminist Criminology 22, 27
[72] Bates n.60

spoke of the obsessive behaviour she undertook as a result of becoming a survivor of revenge porn:

> '"I didn't sleep for months … when this happened in 2010, I would pop [*sic*] awake, and I would have to check my e-mail address, my work e-mail address, my Facebook page, I had this ritual, and I would have to perform this ritual. I'd check eBay, I'd Google my name, you know, the same thing. 1, 2, 3, 4, 5, 6, 7 … I had to do these things. I'd do them three or four times, and be able to go back to sleep. But then I'd wake up."'[73]

Revenge pornography can alter a person's life dramatically which has been the main driving force for its criminalisation across the globe.[74]

In 2014 a debate was held in Westminster Parliament examining the possibility of the creation of a specific criminal offence prohibiting non-consensual imagery, following the likes of several States in America criminalising this form of behaviour.[75] During the debate arguments were put forward that the concept of revenge pornography was already a criminal offence. For instance, the Obscene Publications Act 1959 and 1964 could be used to prosecute individuals who distributed sexually explicit images without consent.[76] Under this Act of Parliament it is a criminal offence to publish an image which may '… deprave and corrupt persons who are likely, having regard to all circumstances, to read, see or hear the matter contained or embodied in it.'[77] Those convicted under the Obscene Publications Act can receive a custodial sentence of up to six months and/or a fine. However, the

---

[73] *Ibid.,* 63-64
[74] Ben Robinson & Nicola Dowling, 'Revenge porn laws "not working", says victims group' *The BBC* (London, 19 May 2019) <https://www.bbc.co.uk/news/uk-48309752> accessed 26 June 2019
[75] HC Deb 19 June 2014, vol 582, col 1374
[76] This was supported in a report conducted by the Communications Committee in 2014. See, Communications Committee, *Social Media and Criminal Offences* (HL 2014-15, 37)
[77] Obscene Publications Act 1959 and 1964 section 1(1)

conditions under the Act means that the image needs to be at its very basic, 'obscene'.

Revenge porn is not always considered obscene due to the imagery or video being considered something likely to be part of mainstream society today.[78] Therefore, if the image can be regarded as mainstream there would be no offence under the Obscene Publications Act. Other Acts which were considered to be applicable to revenge porn prosecutions included the Protection from Harassment Act 1997, the Malicious Communications Act 1988 and the Communications Act 2003. It was put forward that these Acts of Parliament all criminalised the conduct of revenge pornography.[79]

Despite the stance taken by some politicians that revenge pornography was already criminalised, Martin Horwood MP disputed this argument:

> 'I am afraid I am going to go a little further than the right hon. Member for Basingstoke (Maria Miller) and say that nothing I have heard suggests that there are any laws that can be used in a situation when, for instance, the image has not been hacked, the person is an adult, the photos are not grossly offensive- because they were probably taken in a private context originally- and Google, or whichever search engine transmits them through links, does not intend to cause offence. There do not seem to be any legal remedies among the Acts the Minister has mentioned [*sic*] ...'.[80]

Following this debate and further pressure from non-government organisations,[81] the behaviour of revenge pornography was specifically

[78] Gillespie n.61, 876
[79] HC Deb 19 June 2014, vol 582, col 1370
[80] HC Deb 19 June 2014, vol 582, col 1373-1374
[81] Holly Jacobs, 'This is what it is like to be the victim of revenge porn, and why we need to criminalise it' *The Telegraph* (London, 13 February 2015) <http://www.independent.co.uk/voices/comment/this-is-what-it-is-like-to-be-the-victim-of-revenge-porn-and-why-we-need-to-criminalise-it-10045067.html> accessed 12 February 2018

criminalised under section 33 of the Criminal Justice and Courts Act. The first conviction for revenge pornography came around four months' after its prohibition.[82]

Section 33 of the Criminal Justice and Courts Act now makes it a specific criminal offence:

> '… for a person to disclose a private sexual photograph or film if the disclosure is made without the consent of an individual who appears in the photograph or film; with the intention of causing that individual distress.'

The Act gives the justice system a wider interpretation in relation to private and sexual imagery compared to the Obscene Publications Act and other Acts, which were used prior to the changes in the law.[83] The *actus reus* of the offence consists of several elements. First, the defendant must 'disclose a private sexual photograph or film'. Here it is considered that '[a] person "discloses" something to a person if, by any means, he or she gives or shows it to the person or makes it available to the person.'[84]

Second, to satisfy the *actus reus* of section 33 the image must be both private and sexual. Section 35(2) of the Act defines private as '… something that is not of a kind ordinarily seen in public', though the picture itself does

---

[82] *R v Jason Asagba* Reading Magistrates' Court 1 September 2015 (unreported). See also, Siobhan Fention, 'Revenge porn laws: First person found guilty under new laws to be sentenced today' *The Independent* (London, 7 August 2015) <http://www.independent.co.uk/news/uk/crime/revenge-porn-laws-first-person-found-guilty-under-new-laws-to-be-sentenced-today-10444898.html> accessed 19 October 2016

[83] Gillespie n.61, 876

[84] The Criminal Justice and Court Act 2015 section 34(2). The law has adapted to cover 'availability' to include modern technology, as demonstrated in *R v Dooley (Michael)* [2005] EWCA Crim 3093, [2006] 1 W.L.R. 775*,* where it was held that the storing of indecent images of children on a shared networked computer file, amounted to 'availability'. Arguably, this approach would also apply to the law criminalising revenge pornography.

not have to be taken in a private setting.[85] Whereas, an image is considered sexual if it falls into one of the following three categories:

> '… it shows all or part of an individual's exposed genitals or pubic area; it shows something that a reasonable person would consider to be sexual because of its nature; or its content, taken as a whole, is such that a reasonable person would consider it to be sexual.'[86]

The CPS guidelines on prosecuting the offence of disclosing private sexual photographs and films makes it clear that images which are regarded as sexually provocative, may well fall within the second category of what is deemed sexual.[87]

However, the law has been limited to exclude altered images:[88]

> 'The photograph or film is not private and sexual if … it is only by virtue of the alteration or combination mentioned in subsection (4) that the person mentioned in section 33(1)(a) and (b) is shown as part of, or with, whatever makes the photograph or film private and sexual.'[89]

With advances in technology, photos can be easily altered to present to a third party an image which replicates a real-life scenario, which in some cases has been used to abuse and torment others online. In 2014 Zoe Quinn a gamer[90] and journalist, had to flee her home after receiving death and rape threats online following her publicly speaking out about how female gamers

---

[85] Alisdair A. Gillespie, '"Trust me, it's only for me": "revenge porn" and the criminal law' (2015) 11 Criminal Law Review 866, 869

[86] The Criminal Justice and Courts Act 2015 section 35(3)

[87] The Crown Prosecution Service, 'Revenge Pornography - Guidelines on prosecuting the offence of disclosing private sexual photographs and films' (*CPS.gov*, 2018) <http://www.cps.gov.uk/legal/p_to_r/revenge_pornography/> accessed 12 December 2017

[88] This issue was further highlighted by the Law Commission, See, Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018) [10.171]

[89] The Criminal Justice and Courts Act 2015 section 35(5)c

[90] Though there is no true definition of a gamer, Desborough suggests '[a] gamer is an engaged, active, interested and knowledgeable member of the gaming community for whom gaming is a primary hobby.' See, James Desborough, *Inside Gamergate: A Social History of the Gamer Revolt* (Lulu.com 2017) 24

were treated in the gaming industry.[91] Included in this misogynistic abuse were explicit photos of Ms Quinn which had been altered to show her in compromising sexual encounters, many of these images being linked to her ex-partner. One particular image, which was shared across the Internet was of Ms Quinn on all fours, undressed with semen across her chest.[92] Though the image was altered, because of the advances in technology it was difficult for individuals to distinguish that the image was in fact fake. Though this case occurred in America, it is a prime example of conduct which was essentially conducted for revengeful purposes, which would not be covered under section 33 of the Criminal Justice and Courts Act in the UK.[93] Subsequently, online abuse, in particular, revenge porn is becoming a feminist issue.[94]

The final part of the *actus reus* which must be satisfied is that the image must be disclosed without the consent of the person in the picture. For instance, uploading a sexually explicit photo to a social media site, without consent, would satisfy this part of the *actus reus*. In cases which have come

[91] Keith Stuart, 'Zoe Quinn: "All Gamergate has done is ruin people's lives"' *The Guardian* (London, 3 December 2014) <https://www.theguardian.com/technology/2014/dec/03/zoe-quinn-gamergate-interview> accessed 12 December 2017
[92] Anastasia Powell & Nicola Henry, *Sexual Violence in a Digital Age* (Springer 2017) 169
[93] The CPS guidelines on social media offences implies that this behaviour could be covered under other Acts of Parliament. See, The Crown Prosecution Service, 'Guidelines on prosecuting cases involving communications sent via social media' (*CPS.gov*, 2016) <https://www.cps.gov.uk/legal-guidance/guidelines-prosecuting-cases-involving-communications-sent-social-media> accessed 10 January 2018. See also, Alexandra Sims, 'Trolling, Abuse, Sexting and Doxxing all targeted in ambitious new legal guidelines' *The Independent* (London, 10 October 2016) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/online-abuse-internet-sexting-doxxing-trolling-new-legal-guidelines-crime-prosecution-service-a7353536.html> accessed 12 February 2018
[94] Emma A Jane, 'Online Misogyny and Feminist Digilantism' (2016) 30(3) Journal of Media and Cultural Studies 284

before the courts this has been self-explanatory with little evidence that anyone has disputed this part of the *actus reus* in a matter.[95]

The *mens rea* for a breach of section 33 of the Criminal Justice and Courts Act is one of intent. Essentially, it must be found that a person disclosed the private and sexual image intending to cause distress to the individual displayed in the image. For instance, in *R v Clayton Kennedy*[96] the defendant uploaded an explicitly sexual image of his ex-partner on Facebook, intending to cause an 'emotional impact on the victim.'[97] The Act imposes a strict test when establishing an intention to cause distress:

> 'A person charged with an offence under this section is not to be taken to have disclosed a photograph or film with the intention of causing distress merely because that was a natural and probable consequence of the disclosure.'[98]

Therefore, the Act entails that a positive requirement for intent is found.[99] Ledward and Agate state that in most cases:

> '… intent is fairly evident, with many offenders admitting that they posted the images in retaliation for a perceived wrongdoing by the victim. To date, surprisingly few cases are emerging where the alleged offender has relied on the absence of intent in their defence.'[100]

This narrow approach to the law differs from the suggestion put forward by Mitchell as discussed previously. She argued that the *mens rea* for revenge pornography should include not only intention but also recklessness to

---

[95] Jocelyn Ledward & Jennifer Agate, '"Revenge porn" and s.33: the story so far' 28(2) Entertainment Law Review 40, 41
[96] *R v Clayton Kennedy* Cardiff Magistrates Court 6 July 2015 (unreported)
[97] *Ibid.,* per magistrate Dr Chantal Nichol. See, The BBC 'Cardiff man sentenced for "revenge porn" post' *The BBC* (London, 6 July 2015) <http://www.bbc.co.uk/news/uk-wales-south-east-wales-33414500> accessed 15 May 2018
[98] The Criminal Justice and Courts Act 2015 section 33(8)
[99] Ledward & Agate n.95, 41
[100] *Ibid.,*

ensure full protection for victims of this form of abuse. Arguably the term 'reckless' was excluded from section 33 of the Criminal Justice and Courts Act, for fear of over-regulation.[101]

The *mens rea* for revenge pornography is therefore restricted. If it can be found that an individual uploaded an indecent image for anything other than to cause distress, even if the victim was distressed, no criminal offence would have occurred under section 33 of the Criminal Justice and Courts Act. Consequently, the law governing revenge pornography does not criminalise the actions of uploading or disclosing an image for sexual gratification or financial gain.[102]

Revenge pornography can have a significant effect on the victim, which was further reflected in a statement issued by Alison Saunders former Director of Public Prosecutions for the CPS:

> 'Revenge pornography is a particularly distressing crime for the victim, which is often, but not always, brought about by the vengeful actions of former partners. It is a violation of trust between two people and its purpose is to publicly humiliate.'[103]

Consequently, the criminal justice system has attempted to take a robust approach to criminalising the conduct of revenge porn.[104] Following the first

---

[101] Tyrone Kirchengast, 'The Limits of the Criminal Law and Justice: "Revenge Porn" Criminalisation, hybrid responses, and the ideal victim' (2016) 2 UniSA Student Law Review 96, 98

[102] Dr Samantha Pegg, 'Wrong on "revenge porn"' (2015) The Law Society Gazette <https://www.lawgazette.co.uk/comment-and-opinion/wrong-on-revenge-porn/5046957.article> accessed 13 December 2017

[103] The Crown Prosecution Service, 'Man sentenced for "Revenge Porn" – Reading' (*CPS.gov*, 2015) <http://www.cps.gov.uk/thames_chiltern/cps_thames_and_chiltern_news/man_sentenced_for__revenge_porn____reading/> accessed 19 October 2016

[104] Ledward & Agate n.95, 42

year of the Criminal Justice and Courts Act being implemented into the legal system, 206 individuals were prosecuted under section 33 of the Act for disclosing private sexual images.[105] By the end of 2017 this had increased to 465.[106] However, research undertaken by '5 Live', supported by the Revenge Porn Helpline, has highlighted the continuing issues of section 33 of the Criminal Justice and Courts Act. Figures obtained by 5 Live from 19 police forces in England and Wales exposed that the number of police investigations into revenge porn had more than doubled between 2015 and 2019. Yet the number of charges during the same period for revenge porn related offences dropped by 23%. The Revenge Porn Helpline has been heavily critical of the law's response to revenge pornography, going as far as arguing that 'revenge porn laws are not fit for purpose'.[107] Further issues were also raised about the lack of police training following a study conducted by the University of Suffolk in 2017. This uncovered that 95% of 783 police officers, who took part in a survey, had not received training on revenge porn legislation;[108] despite the success advocated by the CPS on prosecutions for revenge pornography in their annual report examining violence against women and girls in 2017.[109]

The studies above illustrate the continued issue of revenge pornography across England and Wales. Social media has been paramount in the

[105] The BBC, 'Revenge porn: More than 200 prosecuted under new law' *The BBC* (London, 6 September 2016) <http://www.bbc.co.uk/news/uk-37278264> accessed 12 February 2018
[106] The Crown Prosecution Service, 'Violence against women and girls report: tenth edition' (*CPS.gov*, 2017) 17 <https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2017.pdf> accessed 30 January 2018
[107] Robinson & Dowling n.74
[108] *Ibid*.,
[109] The Crown Prosecution Service n.106, 1

distribution of revenge porn, as exposed by a BBC Freedom of Information request in 2016. As outlined in chapter one, the BBC exposed that between April 2015 and December 2015 there were 1,160 reports of revenge porn related incidences to police forces across England and Wales.[110] Of the 1,160 reports made to the police, 68% of the perpetrators in these matters used Facebook to expose explicit images of their victims, 12% used Instagram and 5% used Snapchat.[111] For instance, David Jones from the Merseyside area used social media sites to post explicit pictures of his ex-girlfriend.[112]

Despite the prevalence of social media in cases of revenge pornography, under section 33 of the Criminal Justice and Courts Act social media companies, like Facebook and Twitter, are not under a legal obligation to remove revenge pornography.[113] Instead, the law currently relies on social media companies having their own policies in place to remove such content:

> 'Finally, the social media and ISPs need to play their part. They should improve their policies, respond so that people can use their services safely and ensure that, when images are posted that should not be, there are clear ways to take action.'[114]

However, social media companies have created not only their own policies but also their own rules when it comes to revenge pornography. In 2017 the Guardian newspaper obtained Facebook's policies on sexual content,

---

[110] Peter Sherlock, 'Revenge pornography victims as young as 11, investigation finds' *The BBC* (London, 27 April 2016) <http://www.bbc.co.uk/news/uk-england-36054273> accessed 12 February 2018
[111] *Ibid.,*
[112] *R v David Jones* Liverpool Magistrates 19 August 2015 (unreported). See also, The BBC, 'Wallasey man jailed for posting "revenge porn" images' *The BBC* (London, 19 August 2015) <http://www.bbc.co.uk/news/uk-england-merseyside-33992110> accessed 28 April 2017
[113] The Crown Prosecution Service n.87
[114] HC Deb 19 June 2014, vol 582, col 1370

terrorism and violence posted on its site, including revenge pornography.[115] Facebook indicates that revenge pornography will only be removed from its site if three conditions are met:

> '[The] [i]mages [are] produced in a private setting; AND [the] [p]erson in image is nude, near nude, or sexually active; AND [l]ack of consent confirmed by: [v]engeful context (e.g. caption, comments, or page title), OR [i]ndependent sources (e.g. media coverage, or LE [local authority] record [*sic*].'[116]

For Facebook, all three of these conditions have to be found for an image or video to be removed, in which staff have, in some instances around ten seconds to make a decision.[117] Consequently, images uploaded for revengeful purposes may not always be removed by Facebook. For instance, if the image in question has been created in a public place and there is no indication in the caption that the photo has been uploaded as an act of revenge, it will not be considered as breaching Facebook's revenge porn policies.[118]

Due to the lack of response by social media sites in relation to revenge pornography, victims of this form of abuse must rely on section 33 of the Criminal Justice and Courts Act to take action against the perpetrator of this behaviour. Nonetheless, the provision is not without fault. Arguments have recently been put forward that victims of revenge pornography should be

[115] Nick Hopkins, 'Revealed: Facebook's internal rulebook on sex, terrorism and violence' *The Guardian* (London, 21 May 2017) <https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence> accessed 13 February 2018
[116] *Ibid.,*
[117] *Ibid.,*
[118] For a further discussion regarding Facebook's revenge porn policies, see chapter three.

entitled to anonymity under the law, as the actions and consequences of revenge porn are similar to a sexual assault:

> 'The publication of a complainant's name may only compound a painful invasion into privacy that has already been suffered by the disclosure of any intimate sexual images. Moreover, there is currently no mechanism for the effective removal of these images when posted online, and drawing attention to them by publishing the names of complainants redoubles the humiliation.'[119]

In England and Wales victims of certain sexual offences are unable to be identified or have information released about them which may lead to their identification, as they have lifelong anonymity under the Sexual Offences (Amendment) Act 1992. However, this does not apply to section 33 of the Criminal Justice and Courts Act, despite the sexual nature of the offence, as it is currently considered a communications offence.[120] Ex-policing minister Mike Penning argued that the act of revenge pornography mirrors that of blackmail, and consequently should not be put on the same statutory footing as sexual offences:

> '… the offence [the disclosure of photographs and/or films without the consent of the person appearing in them] is more *akin* to the existing malicious communications offence or to blackmail than it is to a sexual offence.'[121]

Despite the stance taken by Penning, research conducted by ICM has exposed that 75% of those surveyed[122] believed that anonymity should be given to revenge porn victims:

> 'Automatic anonymity for all victims of image-based sexual abuse is vital in the interests of justice to ensure increased reporting and

---

[119] Pegg n.102
[120] Robinson & Dowling n.74
[121] This comment was made by the ex-policing minister Mike Penning. See, Ledward & Agate n.95, 41
[122] In total 2048 took part in the study. See, Sandra Laville, '"Revenge Porn" victims should get anonymity, say 75% of people' *The Guardian* (London, 19 July 2016) <https://www.theguardian.com/law/2016/jul/19/revenge-porn-victims-should-get-anonymity-say-75-per-cent-of-people> accessed 20 March 2018

> prosecutions. We know that victims are reluctant to report this pernicious crime to the police because they fear their images or videos going viral on the Internet.'[123]

Arguments have been put forward that section 33 of the Criminal Justice and Courts Act should include anonymity for victims.[124] Currently, in cases of revenge pornography, victims can be publicly named in a court of law and in some cases in the media, this can result in some individuals not reporting the matter to the police for fear that others may be inclined to search for the image online.[125]

There are also issues with how section 33 of the Criminal Justice and Courts Act has been drafted. As previously mentioned a narrow approach is given to the *mens rea* of the offence: 'It is an offence for a person to disclose a private sexual photograph or film … with the intention of causing that individual distress.'[126] Here, for an offence to be committed it must be found that the person who disclosed the image did this with the intention to cause distress. If this element is missing, an offence has not occurred under this Act of Parliament.[127] Consequently, the Act misses the opportunity to criminalise other reasons why an individual may upload a sexually explicit image, such as that of financial gain.

In addition, a narrow meaning has also been given to the term 'sexual material'. The law has been constructed to only cover images which can be

[123] *Ibid*., per Professor Clare McGlynn
[124] Robinson & Dowling n.74
[125] *Ibid.,*
[126] Criminal Justice and Courts Act 2015 section 33(1)b
[127] There is a possibility that the defendant can be prosecuted under another Act of Parliament. For example, the Communications Act 2003.

considered as something not normally seen in public, it exposes a person's genitals, or the reasonable person would come to the decision that the image was sexual. This leaves difficulties in prosecuting those who publish an image to a third party which may not be considered as sexual in today's climate:

> 'Cases in which victims are depicted in their underwear (but the pictures aren't of a sexual nature or don't feature sexual actions) are unlikely to be considered for prosecution.'[128]

The distribution of a photo of an individual in their underwear may well cause the person distress, but if it cannot be considered a sexual image, then no offence would have occurred under section 33 of the Criminal Justice and Courts Act.[129]

Despite issues with the law it can be considered as a positive step forward that the law has expanded to specifically criminalise revenge porn. Revenge pornography has statutory protection that no other form of online abuse has been given, despite its effects having similar consequences to other conducts carried out with the aid of social media.

Chapter Overview

Both the Computer Misuse Act and section 33 of the Criminal Justice and Courts Act have been created from a technology perspective and can be seen to conform to the principles of legality. These legal provisions are clear

[128] Antoinette Raffaela Huber, 'Revenge porn law is failing victims – here's why' *The Conversation* (London, 25 January 2018) <https://theconversation.com/revenge-porn-law-is-failing-victims-heres-why-90497> accessed 16 March 2018

[129] In late June 2019 it was announced that the Law Commission would review revenge porn laws.

in their application and uphold the concepts of foreseeability and accessibility.

The Computer Misuse Act governs three types of conducts: computer hacking, hacking with the intent to cause a further criminal offence and denial of service attacks. As demonstrated above the Computer Misuse Act can be utilised in a social media context, but only in limited circumstances. Yet there is currently no reference to the Computer Misuse Act in the CPS guidelines on social media prosecutions.

Like that of computer misuse, revenge pornography has been made a specific criminal offence under section 33 of the Criminal Justice and Courts Act. Here, it is now illegal to upload a sexually explicit photo of another with the intention to cause the individual distress. Though this has been a positive step forward by the criminal justice system, issues remain with the construction of the law. For example, the Act does not provide anonymity for victims of this form of abuse or cover the conduct of altered images. Regardless of the flaws that can be found within the Act, the statutory footing given to the prohibition of revenge pornography is a positive change implemented by Parliament.

The following chapter will examine in detail two further technology-based provisions, the Malicious Communications Act 1988 and the Communications Act 2003, alongside the CPS guidelines on prosecuting

social media offences. In recent years, these two Acts of Parliament have become paramount in prosecuting social media related offences.

Chapter Five: Recommendations

- The inclusion of the Computer Misuse Act 1990 in the CPS social media prosecuting guidelines;
- Better training for law enforcement to ensure the Computer Misuse Act 1990 is fully understood within the criminal justice system;
- Adapt section 33 of the Criminal Justice and Courts Act 2015 to expand the *mens rea* of the offence to include recklessness;
- Expand the definition of ‘sexual imagery’;
- Prohibit revenge pornography in the form of fake images or videos; and
- Ensure anonymity is given to victims of revenge pornography.

Chapter Six

Social Media, Criminal Law Regulation and Technology-Based Legislation: Part Two

> 'Grossly offensive messages do not contribute much to improving our knowledge or participation as citizens in a democracy. Rather, their effect is to distort communications.'[1]

Like that of the Computer Misuse Act 1990 and section 33 of the Criminal Justice and Courts Act 2015, the Malicious Communications Act 1988 and section 127 of the Communications Act 2003, govern technology-based offences. Though the Malicious Communications Act was originally enacted to govern all forms of communications, except those conducted electronically, the Act was updated to reflect online exchanges in 2001.[2] Both the Malicious Communications Act and section 127 of the Communications Act have become significant legal provisions in prosecuting social media abuse.

Where a complaint about behaviour online does not fall under a specific type of conduct, for instance harassment, stalking or revenge pornography, it can be considered a somewhat miscellaneous offence. Consequently, the behaviour may likely be prosecuted under one of two legal provisions: the Malicious Communications Act or section 127 of the Communications Act.

Parts of this chapter have been published in the Journal of Media Law. See, Laura Bliss, 'The crown prosecution guidelines and grossly offensive comments: an analysis' (2017) 9(2) Journal of Media Law 173

[1] Thomas Gibbon, 'Case Comment: Grossly offensive communications' (2006) 11(4) Communications Law 136, 138 (note)

[2] Criminal Justice and Police Act 2001 section 43

These two provisions are often used to cover trolling online[3] and are associated with offensive language that generally '… becomes a problem only when it is foisted on a recipient who may find it objectionable.'[4]

In an ever-growing technology-based world, individuals are increasingly turning to the likes of Facebook and Twitter to vent their frustrations, often leaving what has become known as a digital trace:[5]

> '[T]wenty years ago where a person made a racist remark in a social setting, the chances of the police ever hearing about it were small. Now a recipient can direct the police to the statement made online and allow them to witness it first hand.'[6]

Comments made online can be readily searched for by third parties, meaning in many cases the statement goes beyond the creator's original audience.[7] The issue for the criminal justice system is in establishing when a person's online message goes from one intended as a joke to one so grossly offensive that it warrants criminalisation.

The following discussion will outline both the Malicious Communications Act and section 127 of the Communications Act, taking into account the mischief behind their implementation. A comparison of the differences between the two provisions will be made before examining in detail the conduct criminalised under both legal provisions. In later parts of this discussion the

---

[3] Sarosh Khan, 'Can the trolls be put back under the bridge?' (2013) 19(1) Computer and Telecommunications Law Review 9, 10
[4] Gibbon n.1, 137
[5] A digital trace can be defined as 'data produced by people while interacting with digital services.' See, Andreas Jungherr *et al*, 'Digital Trace Data in the Study of Public Opinion: An Indicator of Attention Toward Politics Rather Than Political Support' (2017) 35(3) Social Science Computer Review 336, 336-337
[6] Jacob Rowbottom, 'To rant, vent and converse: protecting low level digital speech' (2012) 71(2) Cambridge Law Journal 355, 367
[7] *Ibid.,* 365

Crown Prosecution Service (CPS) guidelines on social media prosecutions will be examined.

Malicious Communications Act 1988

Since 1935 the criminal law has been used to regulate communications which were considered as inappropriate.[8] The most significant change to communication law came in 1988 with the enactment of the Malicious Communications Act. The purpose of the Act was '… to make provision[s] for the punishment of persons who send or deliver letters or other articles for the purpose of causing distress or anxiety.'[9]

Before the change in the law in 1988, issues arose in relation to poison pen letters. Poison pen letters are considered:

> 'a communication, written or otherwise, which is grossly offensive, or of an indecent, shocking, or menacing character, [which was sent] for the purpose of causing needless anxiety or distress [to the recipient] or any other person.'[10]

Many of these letters, though distressing on behalf of the receiver, fell outside the criminal law.[11] For instance, under section 11 of the Post Office Act 1953 it was an offence to send:

> '… any indecent or obscene print, painting, photograph, lithograph, engraving, cinematograph film, book, card or written communication, or any indecent or obscene article whether similar to the above.'

[8] For example, the Post Office (Amendment) Act 1935. See also, Alisdair A. Gillespie, 'Offensive communications and the law' (2006) (17)8 Entertainment Law Review 236
[9] Malicious Communications Act 1988
[10] Law Commission, *Report on Poison-Pen Letters* (Law Com No 147, 1985) [2.1]
[11] Graeme Broadbent, 'Malicious Communications Act 1988: human rights' (2007) 71(4) Journal of Criminal Law 288

Problems occurred in relation to the terms, indecent and obscene. If the material was considered to fall outside the realms of indecent or obscene, no criminal offence had occurred under the Act.[12] For example, the case of a coffin being sent through the postal system, though distressing upon the recipient, was considered as being beyond the scope of the Post Office Act.[13] The gap in the law became even more significant for the criminal justice system when attempting to prosecute poison pen letters.

In 1981 eight men were killed when their lifeboat went missing off the Cornish Coast.[14] After this event occurred, some of the widows of those who lost their husbands in the disaster received poison pen letters.[15] It was found that the letters sent to the widows were indeed grossly offensive and caused harm upon those who received them, but at the time this was not an offence under the law.[16] As a result of this and other failures in the law to protect victims of this form of abuse, the Law Commission issued a report examining the criminal law framework and poison pen letters.

The report conducted in 1985 found that there was a small but significant gap in the law whereby communications sent which were grossly offensive, fell outside the realms of criminal law intervention.[17] Indeed, threats to injure

[12] Law Commission n.10, [2.8]
[13] HC Deb 12 February 1988, vol 127, col 620
[14] Shannon Hards, 'The Penlee Lifeboat disaster happened 36 years ago today - we remember the heroes of the Solomon Browne' *CornwallLive* (Truro, 19 December 2017) <https://www.cornwalllive.com/news/cornwall-news/penlee-lifeboat-disaster-happened-36-945008> accessed 18 April 2018
[15] Broadbent n.11, 289
[16] HC Deb 12 February 1988, vol 127, col 615
[17] Broadbent n.11, 288

a person were not illegal in the criminal law framework of the 1980s.[18] If the communication could have been considered as defamatory this would be contrary to law. The Law Commission found that in many cases the comments being communicated did not defame the victim.[19]

During the consultation period conducted by the Law Commission, emphasis was placed on the types of communications which should be criminalised under the law. It was clear that there was an intention to cover letters, sent *via* both the postal system and sent privately to individuals which were '… grossly offensive, or of an indecent, obscene or menacing character which caused distress or anxiety on the victim.'[20] Concerns arose however as to how far the law should go? The Law Commission discussed in detail examples of items which could be sent in the post that would cause distress or anxiety upon another. For instance, a tape containing grossly offensive material or human faeces. The Law Commission concluded that the law should extend to cover letters and articles which were considered either grossly offensive, indecent, obscene or of a menacing character. The Law Commission decided that electronic communications, such as those sent online would not be covered under the draft Bill they proposed:

> 'The offence will therefore exclude other forms of communication, such as those effected by oral means, by radio, telephone or other forms of electronic communication.'[21]

Therefore, when the Malicious Communications Act was first enacted electronic communications, such as messages sent online, were not covered

[18] Law Commission n.10, [2.11]
[19] *Ibid.,* [1.2]
[20] *Ibid.,* [4.1]
[21] *Ibid.,* [4.7]

under this Act of Parliament. This was amended under section 43 of the Criminal Justice and Police Act 2001 following the increase in the use of technology within society.

The Malicious Communications Act makes it an offence to send:

> '(a) a letter, electronic communication or article of any description which conveys - (i) a message which is indecent or grossly offensive; (ii) a threat; or (iii) information which is false and known or believed to be false by the sender; or (b) any article of electronic communication which is, in whole or part, of an indecent or grossly offensive nature …'.[22]

The *actus reus* consists of two elements. First, the conduct must either be considered a letter, electronic communication or an article which is sent to another. Electronic communication is defined in section 2A of the Act as:

> '(a) any oral or other communication by means of an electronic communications network; and (b) any communication (however sent) that is in electronic form.'

Therefore, messages sent with the aid of social media would constitute an electronic communication. Whereas an article takes a very broad definition and is defined under the Obscene Publications Act 1959 and 1964 as anything '… containing or embodying matter to be read or looked at or both, any sound record, and any film or other record of a picture or pictures.'[23] For example, broken glass sent through the postal system may well fall under this Act of Parliament if other elements of the offence are satisfied. The actual criminal offence is in the sending of the message, there is no need for the intended message to be received by the recipient. This allows the law to intervene even if the letter, electronic communication or article is intercepted

[22] Malicious Communications Act section 1(1)
[23] Obscene Publications Act 1959 and 1964 section 1(2)

by a third party or the recipient does not receive the intended communication.[24]

The second part of the *actus reus* for an offence to have occurred under the Malicious Communications Act concerns the content of the communication. Here, it must be found that the complained about letter, article or electronic communication falls within at least one of the following categories: indecent or grossly offensive, threatening or false. It is sufficient if only part of the message falls into one of these categories. For example, it does not have to be found that the whole communication was grossly offensive to bring an action under the Malicious Communications Act. How the criminal justice system defines these terms, indecent or grossly offensive, threatening and false will be critically examined in later parts of this chapter.

For the *mens rea* to be established it must be concluded that the purpose on behalf of the sender was to cause anxiety or distress upon the receiver, based upon the context of the case.[25] Though the Act contains no definition of these two terms, it has been found that anxiety is considered as falling just short of a recognised psychiatric illness as affirmed in *Majrowski v Guy's and St Thomas's NHS Trust*.[26] Whereas distress can be defined as 'oppressive and unreasonable behaviour'.[27] Clearly, if a person sends a communication

[24] Law Commission n.10, [4.4]
[25] Malicious Communications Act section 1(1)
[26] *Majrowski v Guy's and St Thomas's NHS Trust* [2005] EWCA Civ 251, [2005] Q.B 848 per Auld LJ [45]
[27] *Ibid.,* per May LJ [82]

for another purpose, for instance as an ill-thought-out joke,[28] no offence will have been committed contrary to this Act of Parliament.

In *Connolly v Director of Public Prosecutions*[29] the defendant was convicted under the Malicious Communications Act for the sending of grossly offensive materials to several pharmacists. Connolly was a Roman Catholic pro-life campaigner and disagreed with pharmacies issuing the morning-after pill to female clients. As a form of protest, she sent pictures of aborted foetuses to three pharmacies that sold the morning-after pill. One of the matters before the court, concerned whether the images had been sent to cause anxiety or distress, or was in fact, a form of lawful protest:

> 'A person who sends an indecent or grossly offensive communication for a political or educational purpose will not be guilty of the offence unless it is proved that his purpose was also to cause distress or anxiety.'[30]

The High Court had to balance Connolly's right to freedom of expression as protected under Article 10 of the European Convention on Human Rights and Fundamental Freedoms, alongside the 'rights of others', which would allow the court to legitimately infringe her right.[31] The images sent to the recipients included a photograph of a deceased 21-week-old foetus with the face and limbs clearly visible. The court came to the judgment that the images were sent to cause anxiety and distress contrary to the Malicious Communications Act.

---

[28] *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin), [2013] 1 WLR 183 per Lord Judge [28]
[29] *Connolly v DPP* [2007] EWHC 237 (Admin), [2008] 1 W.L.R. 276 (DC)
[30] *Ibid.,* per Dyson LJ [9]
[31] The infringement freedom of expression will be examined in detail in the following chapter.

The Malicious Communications Act has also been successful in prosecuting offences facilitated *via* the use of social media. For example, Sean Duffy[32] was given an 18 week custodial sentence for sending indecent and grossly offensive communications *via* Facebook. Duffy trolled several Facebook memorial pages which had been created by the friends and family of deceased individuals, including a page set up in remembrance of Natasha MacBryde.[33] Miss MacBryde took her own life at the age of 15 after being hit by a train. On the Facebook memorial page Duffy posted a video entitled 'Tasha the Tank Engine', which featured Miss MacBryde's face being photo-shopped onto the cartoon character 'Thomas the Tank Engine'. Other pages targeted by Duffy included the remembrance pages of Lauren Drew[34] who had passed away following an epileptic seizure and Hayley Bates[35] who had died in a car accident in 2010.

Since the implementation of the Malicious Communications Act into the legal system of England and Wales, the Act has undergone several changes. Prior to 2015 the Malicious Communications Act created what was a summary only[36] offence, carrying a maximum custodial sentence and limitation period

[32] *R v Sean Duffy* Reading Magistrates' Court 13 September 2011 (unreported)
[33] Ben Moore, 'Facebook internet "troll" Sean Duffy jailed' *The BBC* (London, 13 September 2011) <http://www.bbc.co.uk/news/av/uk-england-14907590/facebook-internet-troll-sean-duffy-jailed> accessed 18 April 2018. See also, The BBC, 'Who, what, why: What laws currently cover trolling?' *The BBC* (London, 20 October 2014) <https://www.bbc.co.uk/news/blogs-magazine-monitor-29686865> accessed 19 February 2019
[34] Steven Morris, 'Internet troll jailed after mocking deaths of teenagers' *The Guardian* (London, 13 September 2011) <https://www.theguardian.com/uk/2011/sep/13/internet-troll-jailed-mocking-teenagers> accessed 18 April 2017
[35] *Ibid.,*
[36] Summary only offences are criminal acts which are triable in the Magistrates' Court. Consequently, the maximum custodial sentence which can be imposed is up to 6 months imprisonment.

of six months.[37] This was raised as an issue before Parliament by Angie Bray MP.[38] In her constituency the police attempted to prosecute an individual under section 15 of the Sexual Offences (Amendment) Act 2003, following an adult male sending sexually explicit pictures to a young female. Yet the prosecution failed because a meeting had not taken place, and therefore no offence had occurred under the Sexual Offences (Amendment) Act. No further action could be taken against the individual as the six month limitation period under the Malicious Communications Act had surpassed.[39]

The limitation period also created problems in relation to malicious communications sent online, as it restricted the amount of time the police could gather evidence to build a case against a defendant.[40] To address the procedural limitations and sentencing restrictions, section 15 of the Criminal Justice and Courts Act 2015 made the Malicious Communications Act an either way offence,[41] increasing the maximum custodial sentence under the Act to two years, reflecting the seriousness of the offence.[42]

The Malicious Communications Act has become a prominent Act of Parliament in governing inappropriate content sent online. Nonetheless, its

---

[37] Limitation periods are 'the time limit in within which the state may prosecute a particular crime.' See, George P. Fletcher, *Basic Concepts of Criminal Law* (Oxford University Press 1998) 10

[38] Ministry of Justice and Lord Faulks QC, 'Lord Faulks QC speech to the Criminal Justice Management Conference' (*Gov.uk*, 25 September 2014) <https://www.gov.uk/government/speeches/lord-faulks-qc-speech-to-the-criminal-justice-management-conference> accessed 18 April 2018

[39] Ministry of Justice, 'Malicious Communications Impact Statement' (*Gov.uk*, 30 May 2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/321285/malicious-communicationss-impact-assessment.pdf> accessed 18 April 2018

[40] *Ibid.,*

[41] An either way offence can be tried either in the Magistrates' Court or the Crown Court.

[42] Ministry of Justice n.39

use has been somewhat limited since the enactment of the Communications Act in 2003. Indeed, nearly all forms of communication-based offences fall within the scope of section 127(1) and (2) of the Communications Act.

Communications Act 2003

Following the turn of the new millennium the use of technology and electronic communications increased dramatically across the globe.[43] Subsequently, a joint committee report was conducted to explore how advancements in technology should be regulated by the law in England and Wales:

> 'We are living at a time of revolution in the ways in which we communicate. The worlds of telephone, broadcasting, mobile communications and the Internet are changing and converging with astonishing speed. Meanwhile, our current regulatory framework was designed for a different age. We need to update the framework of regulation, and put in place a system that recognises the current fast-changing picture and can cope with the inevitability of change in years to come.'[44]

In 2003 Parliament enacted the Communications Act to create legislation to keep pace with changing technology.[45]

The Communications Act had several aims. The Act created The Office of Communications commonly referred to as Ofcom,[46] paved the way for the switch from analogue to digital television broadcasting and ensured universal Internet access. The Communications Act has a wide application under the law covering all forms of modern communications including, though not

[43] Sarah E. Dempsey, 'The Increasing Technology Divide: Persistent portrayals of maverick masculinity in US marketing' (2009) 9(1) Feminist Media Studies 37, 52. See chapter one for a discussion on the increase in Internet usage.
[44] HC Deb 12 December 2000, vol 359, col 481
[45] HC Deb 12 December 2000, vol 359, col 483
[46] Ofcom is discussed in detail in chapter nine.

limited to, email, social media and SMS messaging.[47] Section 127 of the Act, specifically governs the improper use of a public electronics communications network.[48]

In *Director of Public Prosecutions v Collins*[49] the defendant made several phone calls to his local MPs office, leaving racially aggravated comments on an answering machine. Though none of the staff were from an ethnic minority background they were distressed by the context of the messages. Here, it was confirmed by the House of Lords that section 127 of the Communications Act covered all forms of communication including email and the telephone. The Law Lords went further to discuss the purpose of the Communications Act. In the High Court Sedley LJ in his judgment argued that section 127 of the Communications Act was created to protect people from unsolicited messages.[50] This was rejected by the House of Lords. For the Law Lords unsolicited messages were already prohibited under the Malicious Communications Act. In the opinion of the House of Lords the purpose of section 127 of the Communications Act was:

> '… to prohibit the use of a service provided and funded by the public for the benefit of the public for transmission of communications which contravene the basic standards of society.'[51]

[47] Rowbottom n.6, 363
[48] Note, broadcasters are exempt from prosecution under the Communications Act 2003 section 127(4). It has even been suggested that this section of the Act can be used to prosecute two individual's making strong racist comments over the telephone. See *Director of Public Prosecutions v Collins* [2006] UKHL 40, [2006] 1 W.L.R. 2223 per Lord Brown of Eaton-under-Heywood [26-27]
[49] *Ibid.,*
[50] *Ibid.,* [8]
[51] *Ibid.,* [7]

Under section 127(1) of the Communications Act, it is a criminal offence to send:

> '(a) by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or (b) causes any such message or matter to be so sent.'

Whereas section 127(2) prohibits the sending of false messages.[52] Like that of the Malicious Communications Act the offence is in the sending of the message, there is no need for the message to be received. Consequently, the *actus reus* consists of two main elements. First, a message must be sent *via* an electronic communications network, and second, the message sent must be of a grossly offensive or of an indecent, obscene or menacing character or can be labelled as false. Despite the need in changes to the law to help combat issues with the advancements in technology, section 127 of the Communications Act simply mirrored section 43 of the Telecommunications Act 1984.

Before section 127 of the Communications Act came into force, section 43 of the Telecommunications Act made it a criminal offence to send:

> '… by means of a public telecommunication system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.'[53]

The only change made to the law itself was the term 'telecommunication system', which was replaced with the phrase 'electronic communication system', simply allowing the law to extend to cover the Internet, a change

[52] False messages will be discussed in detail in later parts of this chapter.
[53] This section of the Act has been repealed by schedule 19(1) of the Communications Act 2003.

which had already occurred under the Malicious Communications Act in 2001.

However, unlike section 43 of the Telecommunications Act, section 127 of the Communications Act does not contain a specific *mens rea* element.[54] Traditionally criminal acts which lack a definitive *mens rea* are considered strict liability offences.[55] However, using the principles laid out in *Sweet v Parsley*,[56] the courts have substituted a *mens rea* element into section 127 of the Communications Act, arguing that it would be illogical for there to be no *mens rea* present:

> '… Parliament cannot have intended to criminalise the conduct of a person using language which is, for reasons unknown to him, grossly offensive to those to whom it relates, or which may even be thought, however wrongly, to represent a polite or acceptable usage. On the other hand, a culpable state of mind will ordinarily be found where a message is couched in terms showing an intention to insult those to whom the message relates or giving rise to the inference that a risk of doing so must have been recognised by the sender.'[57]

Therefore, for an individual to be held liable for a breach of section 127 of the Communications Act, it must be found that a grossly offensive, menacing, indecent, obscene or false message was sent to another recklessly or with intent, as demonstrated in *R v Darryl O'Donnell*.[58]

---

[54] The *mens rea* which was present under section 43 of the Telecommunications Act 1984 was based on the intention to cause 'annoyance, inconvenience or needless anxiety to another', Telecommunications Act 1984 section 43(1)(b).
[55] For a discussion of strict liability see **chapter two**.
[56] *Sweet v Parsley* [1969] 2 W.L.R. 470, [1970] A.C. 132. The principles created by the House of Lords in the case allows the court to substitute a *mens rea* into an offence where the criminal act is considered a true crime as opposed to a regulatory offence.
[57] *Director of Public Prosecutions v Collins* n.48, per Lord Bingham of Cornhill [11]
[58] *R v Darryl O'Donnell* Londonderry Magistrates Court 29 July 2011 (unreported). See also, The BBC, 'Man fined for Gregory Campbell Facebook comment' *The BBC* (London, 29 July 2011) <http://www.bbc.co.uk/news/uk-northern-ireland-14345649> accessed 29 April 2018

There are some parallels between the Malicious Communications Act and the Communications Act. Both provisions cover similar types of behaviours with similarities in the *actus resus* of the offences. Section 127 of the Communications Act was implemented to control communications sent *via* a public network. Whereas the purpose of the Malicious Communications Act was to prohibit unsolicited messages. Nevertheless, it is not always clear within the law as to why one Act is preferred over that of the other.

Malicious Communications Act v Communications Act

Both the Malicious Communications Act and section 127 of the Communications Act can be regarded as similar. In *Collins* Lord Bingham attempted to distinguish between the two provisions:

> 'First, the object of section 127(1)(a) and its predecessor sections is not to protect people against receipt of unsolicited messages which they may find seriously objectionable. That object is addressed in section 1 of the Malicious Communications Act 1988, which does not require that messages shall, to be proscribed, have been sent by post, or telephone, or public electronic communications network. The purpose of the legislation which culminates in section 127(1)(a) was to prohibit the use of a service provided and funded by the public for the benefit of the public for the transmission of communications which contravene the basic standards of our society. A letter dropped through the letterbox may be grossly offensive, obscene, indecent or menacing, and may well be covered by section 1 of the 1988 Act, but it does not fall within the legislation now under consideration [Communications Act]'.[59]

Whereas the Malicious Communications Act covers all forms of contact including those sent by post, the Communications Act only covers behaviour conducted through electronic communications. However, Lord Bingham does not clarify how the criminal justice system distinguishes which Act of

[59] *Director of Public Prosecutions v Collins* n.48, per Lord Bingham of Cornhill [7]

Parliament should take precedence when it comes to electronic communications. Indeed, Scaife suggests that both Acts have become interchangeable in the legal system of England and Wales.[60]

In July 2011 an individual received a caution under the Malicious Communications Act for sending false information *via* a communications network.[61] The anonymous blogger had made allegations that a contestant on the television show 'Britain's Got Talent' had been groomed for the show by key organisers. The allegations were later proven to be false. Nevertheless, it has been suggested that this matter was pursued under the wrong Act of Parliament, in fact the individual should have been cautioned contrary to the Communications Act.[62]

For an offence to have been committed under the Malicious Communications Act a person must send 'to another a letter, electronic communication or article of any description …'.[63] The key phrase here is 'to another'. Indeed, the discourse of the Act suggests that the communication must be directed at a specific individual. Therefore, this Act of Parliament should only cover offences of private communications rather than public messages. For example, a private inbox message sent *via* Facebook. Consequently, a public post on a blogging site should not fall within this Act of Parliament.[64]

[60] Laura Scaife, *Handbook of Social Media and the Law* (Routledge 2015) 166
[61] Press Association, 'Britain's Got Talent blogger cautioned by police' *The Guardian* (London, 3 July 2011) <https://www.theguardian.com/tv-and-radio/2011/jul/03/britains-got-talent-blogger-cautioned> accessed 1 May 2018
[62] Scaife n.60, 165-166
[63] Malicious Communications Act 1988 section 1
[64] Scaife n.60, 165-166

Under the principle of legality as discussed in chapter two, legal provisions need to be constructed in a clear and precise manner, for an individual to be liable for a criminal offence. In *Kafkaris v Cyprus*[65] the European Court of Human Rights noted that:

> 'An individual must know from the wording of the relevant provision and, if need be, with the assistance of the courts' interpretation of it, what acts and omissions will make him criminally liable and what penalty will be imposed …'.[66]

Though the Malicious Communications Act and section 127 of the Communications Act can be considered as similar provisions, they both carry different sentencing tariffs,[67] therefore certainty is needed. The discourse of the Malicious Communications Act indicates that the Act will only cover private communications, yet it was used to prosecute an online blog in 2011.[68]

The CPS have attempted to overcome this issue in their 2018 social media guidelines by highlighting the key differences between both the Malicious Communications Act, and section 127 of the Communications Act, in particular the difference between the mental elements of the crime. As previously discussed, for an action to be brought under the Malicious Communications Act, the sender of the message must have sent the communication for '… the purpose of causing distress or anxiety.' Whereas

[65] *Kafkaris v Cyprus* App no 21906/04 (ECtHR, 12 February 2008)
[66] *Ibid.,* [140]
[67] The maximum sentence which can be given under the Malicious Communications 1988 is 2 years. Whereas the maximum sentence which can be given under section 127 of the Communications Act 2003 is 6 months.
[68] Press Association n.61

under section 127 of the Communications Act, the sending of the message must be done with 'intent' or 'recklessness' to the sending of a grossly offensive, indecent, false or menacing message. Here, the CPS, through the analysis of the discourse of the provisions, highlights that a higher evidential threshold test will be applied to matters pursued under the Malicious Communications Act:[69]

> 'Section 1 [Malicious Communications Act] requires the sending of a letter, electronic communication or article of any description to another person. Depending on the facts of the case, a social media communication which is merely a blog or a comment posted on a website may not suffice as sending to another. Prosecutors should consider the evidence that the communication was addressed (either by name or in terms) to a specific recipient, and how likely that the specific recipient was to receive it (did they also have a Twitter or Facebook account?) Section 127 [Communications Act] requires only that the message or other matter is sent, and so this will cover the posting of a message, and indeed re-posting or other sharing of a communication.'[70]

By applying the 2018 guidelines the use of the Malicious Communications Act in the case of the 'Britain's Got Talent' blogger, was indeed pursued under the wrong Act of Parliament.

The difficulties in the criminal justice system distinguishing between these two legal provisions mean that individuals can, and have been, pursued under the wrong legal provision, an argument that is also applicable to the Protection from Harassment Act, as discussed in chapter four. In chapter four it was argued that the Protection from Harassment Act was being applied incorrectly, resulting in victims being failed by the law, as law

[69] The Crown Prosecution Service, 'Guidelines on Prosecuting Cases Involving Communications Sent via Social Media' (*CPS.gov,* 21 August 2018) [14] <https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media> accessed 11 October 2018
[70] *Ibid.,*

enforcement regularly misunderstood the differences between harassment, stalking and grossly offensive behaviour. The lack of understanding of the key differences between the Malicious Communications Act and section 127 of the Communications Act can leave victims of online abuse at a disadvantage, whilst also breaching the principle of legality.

It is important to distinguish between the Malicious Communications Act and section 127 of the Communications Act, as both provisions carry different sentencing tariffs. Under section 127 of the Communications Act, a person found guilty of an offence prohibited under this legal provision can receive a maximum custodial sentence of up to six months imprisonment. Whereas under the Malicious Communications Act, an individual can be imprisoned for a term not exceeding two years.[71] It is therefore of paramount importance that both the Malicious Communications Act and section 127 of the Communications Act are clearly distinguished in the criminal justice system.

Types of behaviours criminalised

Under the Malicious Communications Act, it is an offence to send a message which can be categorised as indecent or grossly offensive, a threat, or a message which can be deemed as false. Section 127(1) and (2) of the Communications Act prohibits the sending of a message which is false, grossly offensive, indecent, obscene or of a menacing character. In the discussion below each of these types of conducts will be taken in turn and explained in a social media context.

[71] Note, both provisions also carry a fine.

Indecent

The conduct of sending a communication which is indecent is criminalised under both the Malicious Communications Act and section 127(1) of the Communications Act. Neither Act defines the term indecent. Instead, the courts have come to accept that the term 'indecent' takes its ordinary meaning in a given society and will be subjective depending on the context of a case.[72] Under the principles of legality in the criminal law as discussed in chapter two, legal provisions must be clear and certain so citizens can abide by the law. The idea that the term 'indecent' will be subjective depending on the case before the courts creates uncertainty within the law. This is especially true in matters concerning social media, as what one person may find 'indecent' another may not. However, it can be considered that indecent material goes beyond grossly offensive messages but are not quite obscene communications.[73]

Obscene

Obscene is defined as:

> '… an article [which] … tend[s] to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it ...'.[74]

Here, a matter will be considered to be obscene if the content goes beyond what is acceptable in a multicultural society.[75] Though the term, 'obscene' may be considered as vague, the concept that obscene material is based on

[72] *Director of Public Prosecutions v Collins* n.48, [10]
[73] *Ibid.,* [11]
[74] Obscene Publications Act 1959 and 1964 section 1(1)
[75] *Handyside v United Kingdom* (1976)1 EHRR 737

acceptability in a multicultural society, as opposed to the context of the case like that of the term 'indecent', allows for the law to adapt to the changing nature of society. As Lord Bingham argues:

> 'It is accepted that absolute certainty is unattainable, and might entail excessive rigidity since the law must be able to keep pace with changing circumstances, some degree of vagueness is inevitable and development of the law is a recognised feature of common law courts.'[76]

Indeed, what may have been classified as 'obscene' 30 years ago, may not be today. Despite section 127(1) of the Communications Act prohibiting obscene material, in matters which can be labelled as corrupting and depraving a person the defendant will likely be charged under the Obscene Publications Act,[77] as opposed to section 127(1) of the Communications Act.

In *R v Smith (Gavin)*[78] the defendant had detailed in several online chat rooms[79] explicit fantasies of sadistic sexual acts to conduct on young children. The messages were sent to other individuals who were also taking part in the discussion. Instead of being prosecuted for sending obscene messages contrary to section 127 of the Communications Act, carrying a maximum sentence of 6 months imprisonment,[80] he was prosecuted and convicted under section 2(1) of the Obscene Publications Act, which carries a maximum custodial sentence of up to five years.[81]

---

[76] *R v Rimmington, R v Goldstein* [2005] UKHL 63, [2006] 1 A.C. 459 per Lord Bingham [35]
[77] This Act is discussed further in later parts of this chapter.
[78] *R v Smith (Gavin)* [2012] EWCA Crim 398, [2012] 1 W.L.R. 3368
[79] An internet chat room is similar to a conference held online, where members join to speak to other individuals who may have the same interests as others in the group. See, Peter Reimann, 'Communities in practice' in Heimo H. Adelsberger *et al* (eds), *Handbook on Information Technologies for Education and Training* (2nd edn, Springer 2008) 280
[80] Communications Act 2003 section 127(3)
[81] Obscene Publications Act 1959 and 1964 section 2(1)

False Messages

The Malicious Communications Act and section 127(2) of the Communications Act also prohibits the sending of a message which can be categorised as false. Put simply, a false communication is the sending of a message which contains information which the sender knows to be untrue. For instance as discussed above, the anonymous blogger who was given a caution under the Malicious Communications Act, for his statements surrounding contestants on the reality television show 'Britain's Got Talent'.[82] From an analysis of the CPS guidelines it could be suggested that this behaviour has now been extended to cover fake online profiles.

In recent years, there has been a rise in the use of fake social media accounts created solely to abuse another.[83] For instance, Kirstie Allsopp a Channel 4 presenter, had to approach the police in 2012 after receiving continued sexual threats from two anonymous Twitter accounts. She spoke about being told '… to shoot [her] own womb [and to] bleed to death with a spade in [her] vagina.'[84]

---

[82] Scaife n.60, 165-166

[83] James Titcomb, 'Facebook admits up to 270m users are fake and duplicate accounts' *The Telegraph* (London, 2 November 2017) <https://www.telegraph.co.uk/technology/2017/11/02/facebook-admits-270m-users-fake-duplicate-accounts/> accessed 30 April 2018. In May 2017 Facebook detailed the scale of abuse on its site. Their study found that in one three month period they had removed 583 million fake accounts. See, Dave Lee, 'Facebook details scale of abuse on its site' *The BBC* (London, 15 May 2018) <http://www.bbc.co.uk/news/technology-44122967> accessed 29 May 2018. See chapter one for more details.

[84] Josh Halliday, 'Helen Skelton quits Twitter after abuse from trolls' *The Guardian* (London, 2 August 2012) <https://www.theguardian.com/technology/2012/aug/02/celebrities-quit-twitter-abuse> accessed 30 April 2018

In 2016 following the CPS updating their prosecuting guidelines on social media offences, discussed in later parts of this chapter, emphasis was placed on tackling the growing trend of anonymous online profiles:

> 'Online communication is developing at such a fast pace, new ways of targeting and abusing individuals online are constantly emerging … Offenders can mistakenly think that by using false online profiles and creating websites under a false name their offences are untraceable.'[85]

The statement given by the CPS during the release of the updated guidelines in 2016, proceeded to give examples of behaviours which are criminalised under the law, including the creation of a fake social media profile containing false information. However, the statement stated that this type of conduct is categorised as grossly offensive under the law, as opposed to being classified as false.[86] The 2016 guidelines themselves made very little reference to what constitutes a false message. Instead, the guidelines simply stated that the prosecutor should take into consideration that certain types of behaviours can be considered as false, with little explanation given.[87]

In August 2018 the guidelines were further updated regarding what can constitute a false communication:

> 'The act of setting up a false social networking account or website, or the creation of a false or offensive profile or alias could amount to a criminal offence, depending on the circumstance. For example: [1] The former estranged partner of a victim creates a profile of the victim on a Facebook page, to attack the character of the victim, and the profile includes material that is grossly offensive, false, menacing or

[85] David Barrett, 'Faking social media accounts could lead to criminal charges' *The Telegraph* (London, 3 March 2016) <https://www.telegraph.co.uk/news/uknews/crime/12180782/Faking-social-media-accounts-could-lead-to-criminal-charges.html> accessed 30 April 2018
[86] *Ibid.,*
[87] The Crown Prosecution Service, 'Guidelines on Prosecuting Cases Involving Communications Sent via Social Media' (*CPS.gov,* 2016) <http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/> accessed 10 October 2016

obscene …'.[88]

The CPS supports the idea that false communications can encompass fake online profiles 'depending on the circumstance[s].'[89]

Threatening

The Malicious Communications Act also makes it a criminal offence to convey a message which is threatening. Like that of obscene communications, it is unlikely that this type of message would be prosecuted under this Act of Parliament.[90] Instead, other Acts such as section 16 of the Offences Against the Person Act 1861, which criminalises the conduct of a threat to kill, can be used. The key issue here turns on whether the communication can be considered as a credible threat. If it is regarded as non-credible then it is likely the sender will be charged with an offence of sending either a grossly offensive message or a message of a menacing character.

Menacing Messages

Under both the Malicious Communications Act and the Communications Act no definition of 'menacing' is included, instead it has come to be accepted that a message will be menacing if it can be considered a non-credible threat.[91] The law has to distinguish between a menacing message and a

[88] The Crown Prosecution Service, n.69, [8]
[89] *Ibid.,*
[90] The Crown Prosecution Service n.87
[91] David Allen Green, 'The "Twitter Joke Trial" returns to the High Court' (*NewStatesman*, 22 June 2012) <https://www.newstatesman.com/blogs/david-allen-green/2012/06/twitter-joke-trial-david-allen-green> accessed 30 April 2018. See also, *Director of Public Prosecutions v Collins* n.48, per Sedley LJ [10]

message which can be labelled as a joke or satire humour, even if it is ill-thought-out on behalf of the sender.

On 6 January 2010 Paul Chambers took to Twitter to vent his frustration following the closure of Doncaster Robin Hood Airport due to bad weather: 'Crap! Robin Hood Airport is closed. You've got week [*sic*] and a bit to get your shit together otherwise I'm blowing the airport sky high.'[92] This tweet later came to the attention of airport officials. It was deemed by airport officials that the message was a non-credible threat, and therefore reported to the police rather than the Ministry of Defence.[93]

Foster puts forward several arguments as to why the threat was deemed non-credible by authorities.[94] First, the communication was posted on Twitter for widespread reading, which would be considered as unusual in the context of threatening to blow an 'airport sky high'. Second, when examining the discourse of the tweet, the language and grammar were inconsistent with the intention of terrorism. Last, it would have been unusual for a person to threaten terrorism in such a way which makes the sender so easily identifiable. Consequently, Chambers was arrested and convicted of sending a menacing message contrary to section 127(1) of the Communications Act.[95]

[92] Chambers was due to fly to Northern Ireland to meet with a girl he had met on Twitter.
[93] Alisdair A. Gillespie, 'Twitter, jokes and the law' (2012) 76(5) Journal of Criminal Law 364 (note)
[94] Steve Foster, 'Freedom of expression: is there a human right to make a joke?' (2012) 17(2) Coventry Law Journal 97, 99
[95] *R v Paul Chambers*, Doncaster Magistrates' Court, 10 May 2010 (unreported)

Chambers and his legal team appealed his conviction in the Crown Court[96] arguing that his message was intended as a joke, and therefore he did not have the relevant *actus reus* or *mens rea* needed to commit the offence. This was dismissed by the Crown Court who concluded that the tweet sent by Chambers was 'menacing in its content and obviously so. It could not be more clear. Any ordinary person reading this would see it in that way and be alarmed.'[97] He was later permitted to appeal before the High Court.[98]

The original case heard before the High Court was subjected to a second appeal after an agreement was unable to be reached in the first case.[99] Unlike the finding of the Crown Court, the High Court came to the judgment that Chambers' comments, though 'ill-thought-out', were intended as a joke and as a result quashed his conviction in July 2012:

> 'Satirical, or iconoclastic, or rude comment, the expression of unpopular or unfashionable opinion about serious or trivial matters, banter or humour, even if distasteful to some or painful to those subjected to it should and no doubt will continue at their customary level, quite undiminished by this legislation [Communications Act].'[100]

The judgment of the High Court has been praised with Foster going as far as arguing that the case of *Chambers* was a '… victory for common sense',[101]

[96] *Chambers v Director of Public Prosecutions*, Doncaster Crown Court, 3 March 2011 (unreported). For a discussion of the case history see, Gervase de Wilde, 'News: "Twitter Joke" Case goes to the High Court' (*The International Forum for Responsible Media Blog,* 8 February 2012) <https://inforrm.org/2012/02/08/news-twitter-joke-case-goes-to-the-high-court-gervase-de-wilde/> accessed 2 May 2018
[97] Per Judge Jacqueline Davis found Scaife n.60, 135
[98] *Chambers* n.28
[99] Scaife n.60, 135
[100] *Chambers* n.28, per Lord Judge [28]
[101] Steve Foster, n.94, 101

after many commentators were heavily critical of the criminal justice systems approach to the matter.[102] Indeed, Gillespie states:

> 'Paul Chambers should have been told to be careful about his choice of tweets, but prosecution was unnecessary, especially given that nobody took it seriously.'[103]

It is estimated that the total cost of this case to the taxpayer was around £18,000.[104]

The police, the CPS and the courts need to ensure they effectively distinguish between comments which can be considered as a joke or banter, and messages which can be deemed as menacing. This is even more apparent when it comes to the criminalisation of grossly offensive messages.

Grossly Offensive Messages

Both the Malicious Communications Act and section 127 of the Communications Act prohibits the conduct of sending grossly offensive messages *via* the use of a communications network. Put simply, it is an offence to send a message of a grossly offensive nature *via* all forms of technology under both legal provisions. For the criminal justice system, it is denoting what is meant by the term 'grossly offensive':

> 'Some of us might draw the boundary in one place, whilst others who are particularly concerned about the development of electronic communications might draw it in another.'[105]

---

[102] Lilian Edwards, 'Section 127 of the Communications Act 2003: Threat or Menace?' (2012) 23(4) Computers & Law 22
[103] Gillespie n.93, 368
[104] Nick Cohen, '"Twitter joke" case only went ahead at insistence of DPP' *The Guardian* (London, 28 July 2012) <https://www.theguardian.com/law/2012/jul/29/paul-chambers-twitter-joke-airport> accessed 2 May 2018
[105] Law Commission n.10, [3.6]

In *Collins*, the matter concerning racist comments being left on an answering machine as discussed previously, suggestions were put forward by the judiciary as to what constitutes a grossly offensive message. For Sedley LJ in the High Court, a message can be labelled as grossly offensive when it breaches the '… standards of an open and just multiracial society.'[106] Whereas for Lord Bingham, grossly offensive comments can be defined as '… highly abusive, insulting, pejorative, [and of an] offensive character.'[107] Consequently, there is no true meaning in law as to what constitutes a grossly offensive message, instead 'grossly offensive' is deemed to take its ordinary English meaning.[108]

On 1 October 2012 in Machynlleth Wales, the five year old child April Jones was reported missing by her parents.[109] The case quickly caught the attention of the national press along with her picture being actively shared across social media sites.[110] During the evening of 1 October Matthew Woods from the Lancashire area made several remarks on Facebook in relation to the missing schoolchild, before going on to make comments about Madeleine McCann, a child who went missing in Portugal in 2007. Comments included, 'I woke up this morning in the back of a transit van with two beautiful little girls, I found April in a hopeless place.' 'Could have just started the greatest Facebook argument EVER [*sic*]. April fools, who wants

[106] *Director of Public Prosecutions v Collins* n.48, [11]
[107] *Ibid.,* per Lord Bingham of Cornhill [13]
[108] *Connolly v Director of Public Prosecutions* n.29, per Lord Justice Dyson [10]
[109] Telegraph Reporters, 'What happened to murdered April Jones and who is Mark Bridger?' *The Telegraph* (London, 20 June 2017) <https://www.telegraph.co.uk/news/0/happened-murdered-april-jones-mark-bridger/> accessed 29 April 2018
[110] The following day Mark Bridger was arrested, and later convicted of April's murder.

Maddie? I love April Jones.'[111] He then went on to make sexually explicit comments about the two girls. Because of these messages the next day fifty people descended on Woods' home resulting in the police having to arrest him for his own safety. He was later rearrested for sending grossly offensive messages contrary to section 127(1) of the Communications Act.

During the court hearing, it was argued by his defence team that '[i]n one moment of drunken stupidity he [placed] himself as public enemy number two - behind only the person who carried out this crime.'[112] The chairman of the bench Bill Hudson concluded that the comments made by Woods were so 'abhorrent' that a strong sentence was needed to reflect the severity of the crime. Woods was handed down a prison sentence of 12 weeks.[113]

Whereas a different approach was undertaken in the matter of Daniel Thomas.[114] Thomas, a Footballer, took to Twitter following the divers Tom Daley and Peter Waterfield coming fourth during the 2012 London Olympics: 'if there is any consolation for finishing fourth at least [*sic*] daley and waterfield [*sic*] can go bum each other #teamHIV'. Despite the offensive nature of the comment made by Thomas, it was decided by the CPS that the statement was not so grossly offensive it warranted criminal law intervention:

> 'There is no doubt that the message posted by Mr Thomas was offensive and would be regarded as such by reasonable members of

[111] Steven Morris & Dan Sabbagh, 'April Jones: Matthew Woods jailed over explicit Facebook comments' *The Guardian* (London, 8 October 2012) <https://www.theguardian.com/uk/2012/oct/08/april-jones-matthew-woods-jailed> accessed 29 April 2018
[112] *Ibid.,*
[113] *R v Matthew Woods*, Chorley Magistrates Court, 8 October 2012 (unreported)
[114] The Crown Prosecution News Brief, 'DPP Statement on Tom Daley Case and Social Media Prosecutions' (*CPS.gov,* 2012) <http://blog.cps.gov.uk/2012/09/dpp-statement-on-tom-daley-case-and-socialmedia-prosecutions.html> accessed 29 April 2018

> society. But the question for the CPS is not whether it was offensive, but whether it was so grossly offensive that criminal charges should be brought. The distinction is an important one and not easily made.'[115]

There is a line between offensive and grossly offensive commentary but, it is hard to distinguish when a comment crosses the appropriate threshold to warrant criminalisation. [116] For Lilienthal and Ahmad, the distinction simply falls on whether the reasonable person would find the communication grossly offensive.[117] However, as argued by Gillespie certain sectors of society will always deem a message more grossly offensive than others, bringing issues in prosecuting abusive comments under these legal provisions.[118] Nonetheless, this is disputed by Rowbottom who argues that the current use of section 127 of the Communications Act and the Malicious Communications Act in governing online behaviour can be '… overly expansive and catch statements that might not warrant such serious treatment',[119] which in turn has a chilling effect on free speech.[120] Yet there is no clear distinction as to when a message goes from one being of an offensive nature to one so grossly offensive the criminal law should intervene.

Under the principle of legality:

> '… no one should be punished under a law unless it is sufficiently clear and certain … and no one should be punished for any act which was not clearly and ascertainably punishable when the act was

[115] *Ibid.,*
[116] Laura Bliss, 'The crown prosecution guidelines and grossly offensive comments: an analysis' (2017) 9(2) Journal of Media Law 173, 177
[117] Gary Lilienthal & Nehaluddin Ahmad, 'Hate crime and social media in the UK' (2016) 22(7) Computer and Telecommunications Law Review 188, 191
[118] Gillespie n.8, 237
[119] Rowbottom n.6, 375
[120] *Ibid.,*378

done.'[121]

The matters of *Woods* and Thomas highlight the lack of clarity contained in the Malicious Communications Act and section 127(1) of the Communications Act in terms of what is considered grossly offensive behaviour. Though:

> '[i]t is accepted that absolute certainty is unattainable, and might entail excessive rigidity since the law must be able to keep pace with changing circumstances, some degree of vagueness is inevitable …'.[122]

Yet as potently put by Allen:

> '… in today's new, challenging digital environment, the existing body of legislative instruments, including the Communications Act 2003, do not provide for the degree of harmonisations, clarity nor necessary efficiency to meet the demands which cases such as *Woods* are placing on them.'[123]

The lack of clarity and case examples illustrating grossly offensive material, means mistakes are occurring within the criminal justice system. For instance, the case of *R v Alison Chabloz*[124] illustrates the continued misunderstanding of the term grossly offensive.

Chabloz who defines herself as a holocaust revolutionist published several videos on the social media site YouTube. These videos contained footage of Chabloz performing songs set to the beat of traditional Jewish folk music, which contained anti-Semitic hate. 'Campaign Against Anti-Semitism', a not-for-profit organisation, had made numerous complaints to the police about Chabloz's behaviour online, yet no further action was taken by authorities. In

[121] *R v Rimmington* n.76, per Lord Bingham [33]
[122] *Ibid.,* per Lord Bingham [35]
[123] Green n.91
[124] *R v Alison Chabloz* Westminster Magistrates' Court 11 January 2018 (unreported)

fact, at one-point Chabloz herself approached her local police force claiming she was being harassed online by the Jewish community, leading to the police believing she was a victim of online abuse.[125] Following the lack of action undertaken by authorities, 'Campaign Against Anti-Semitism' chose to pursue a private prosecution against Chabloz, before the CPS eventually took over the prosecution of the defendant.

Westminster Magistrates' Court concluded that Chabloz had committed the offence of sending grossly offensive content contrary to section 127(1) of the Communications Act, a decision later upheld by the Crown Court,[126] with the prosecution successfully arguing that:

> '[t]he songs, specifically the language used within them, have been carefully considered and composed with the language chosen deliberately ... They are anti-Semitic, they are targeting the Jewish people as a whole and use both their content and their tone to ensure maximum offence.'[127]

Yet if it had not been for the private prosecution the limitation period under section 127(1) of the Communications Act would have lapsed, despite there now being social media prosecuting guidelines in place.

The Crown Prosecution Guidelines: Social Media Offences

Following the matter of Thomas and the case of *Chambers*, the CPS announced plans to create and implement prosecuting guidelines on social media related offences.[128] This followed further concerns about the lack of

[125] Laura Bliss, 'Social Media: "A Theme Park just for Fools"' (2018) 82(4) The Journal of Criminal Law 301, 303 (note)
[126] *Alison Chabloz v* Southwark Crown Court 13 February 2019 (unreported)
[127] Bliss n.125, 302
[128] The Crown Prosecution News Brief n.114

consistency within police forces to take the matter of online abuse seriously.[129] The guidelines were released in 2013 later being updated in October 2016 and August 2018.

Like that of other criminal offences, a two-stage test[130] is applied by prosecutors in social media related cases, to establish if a complained about matter is worthy of a recommendation for prosecution. The first stage is known as the evidential test:

> 'When deciding whether there is enough evidence to charge, Crown Prosecutors must consider whether evidence can be used in court and is reliable and credible, and there is no other material that might affect the sufficiency of evidence. Crown Prosecutors must be satisfied there is enough evidence to provide a "realistic prospect of conviction" against each defendant.'[131]

In social media related offences, the CPS must be content that the conduct satisfies the *actus reus* and *mens rea* of an offence governed by law. In the most recent version of the guidelines, Part A lists fifteen specific criminal behaviours which can be conducted with the aid of social media, alongside the Act of Parliament or common law principle that prohibits such conduct.[132] Here, prosecutors must find a clear breach of at least one of these legal provisions contained in the guidelines. The guidelines make it clear that

---

[129] Matthew Weaver, 'Police are inconsistent in tackling online abuse, admits chief constable' *The Guardian* (London, 14 April 2016) <https://www.theguardian.com/uk-news/2016/apr/14/online-abuse-policeinconsistent-digital-crime-stephen-kavanagh> accessed 1 March 2017. See also Alex Bailin QC & Edward Craven, 'Prosecuting social media: the DPP's interim guidelines' (*The International Forum for Responsible Media Blog*, 23 December 2012) <https://inforrm.wordpress.com/2012/12/23/prosecutingsocial-media-the-dpps-interim-guidelines-alex-bailin-qc-and-edward-craven/> accessed 20 July 2017

[130] For all criminal offences the CPS use a two-stage approach, known as the evidential test and the public interest test. See, The Crown Prosecution Service, 'The Code for Crown Prosecutors' (*CPS.gov*, 26 October 2018) <https://www.cps.gov.uk/publication/code-crown-prosecutors> accessed 19 February 2019

[131] *Ibid.,*

[132] The Crown Prosecution Service n.69, [7]

when it comes to offences governed under the Malicious Communications Act and section 127 of the Communications Act, a high evidential threshold will need to be passed before a recommendation for prosecution is made.[133]

For Edwards the high threshold placed on grossly offensive and menacing commentary ensures freedom of expression is not restricted, as endorsed by the CPS prosecuting guidelines on social media related offences.[134] In the previous versions of the guidelines the CPS made it clear that prosecutors must take into account an individual's right to freedom of expression, a factor discussed in more detail in the following chapter, alongside ensuring the communication goes beyond a joke, when determining if a comment or conduct carried out on social media is worthy of prosecution:

> 'Prosecutors are reminded that what is prohibited under section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003 is the sending of a communication that is grossly offensive. A communication sent has to be more than simply offensive to be contrary to the criminal law. Just because the content expressed in the communication is in bad taste, controversial or unpopular, and may cause offence to individuals or a specific community, this is not in itself sufficient reason to engage the criminal law.'[135]

This is a similar approach endorsed in the 2018 version of the guidelines. Yet the guidelines do not refer to other 'rights' which need to be considered when it comes to the protection of victims from abuse online. For example, the right to privacy. As will be discussed in chapter seven, privacy is more than a person's right to a private life, it entails a right not to have your mental

[133] *Ibid.,* [10-15]
[134] Edwards n.102
[135] The Crown Prosecution Service n.87

wellbeing compromised. Online abuse can have a significant effect on a person's mental health, as discussed in chapter one.

The high threshold endorsed by the CPS in matters concerning the Malicious Communications Act and section 127 of the Communications Act, puts pressure on victims and the police to gather substantial evidence that a communications-based offence has taken place. This can be difficult as companies such as Facebook and Twitter are slow in aiding law enforcement as outlined in chapter three, which means in some cases the limitation period has passed before sufficient evidence can be gathered. In addition, as highlighted previously the criminal justice system relies on the self-regulation of social media companies, which is currently inadequate.[136] Further endorsed by Rowbottom who argues:

> 'The difficulty with such self-regulatory measures is that it leaves the private body to decide what standards apply and make a determination about the content.'[137]

The CPS guidelines are consequently a welcomed approach to the governance of online behaviour but are not without fault.[138]

The second stage, which must be satisfied for a recommendation to be put forward by the CPS to prosecute, is that of the public interest element. All cases which are put before the courts must be in the public interest.[139] Put simply, even if the evidential test is met, if a matter can be considered as not

[136] Sarah Birkbeck, 'Can the use of social media be regulated?' (2013) 19(3) Computer and Telecommunications Law Review 83
[137] Rowbottom n.6, 380
[138] Bailin QC & Edward n.129
[139] The Crown Prosecution Service n.87, 7

being in the public interest, the CPS will not support an application for prosecution. Here, several factors are taken into account:[140]

- How likely is the perpetrator to re-offend? Emphasis is placed on distinguishing between individuals who make a one-off comment online, and those who partake in a campaign of abuse;
- The age of the defendant. The guidelines make it clear that if the defendant is under the age of 18 it is unlikely to be in the public interest to prosecute them for social media related offences;
- Did the suspect express genuine remorse? If the suspect expresses genuine remorse it is unlikely that a recommendation for prosecution will be put forward. Similarly, if the perpetrator removes the offending communication quickly it is unlikely to be in the public interest to prosecute;
- Who was the communication aimed at? Communications which were never intended for a wide audience may result in a decision not to prosecute;
- Does the communication contain a hate crime element; and
- 'The circumstances of and the harm caused to the victim ...'.[141]

The CPS will evaluate all these factors before deciding if a matter should be presented before the courts. However, like that of the evidential test the guidelines state that '… in many cases a prosecution is unlikely to be … in the public interest.'[142]

[140] The Crown Prosecution Service n.69, [31]
[141] *Ibid.,* [31]
[142] The Crown Prosecution Service n.87

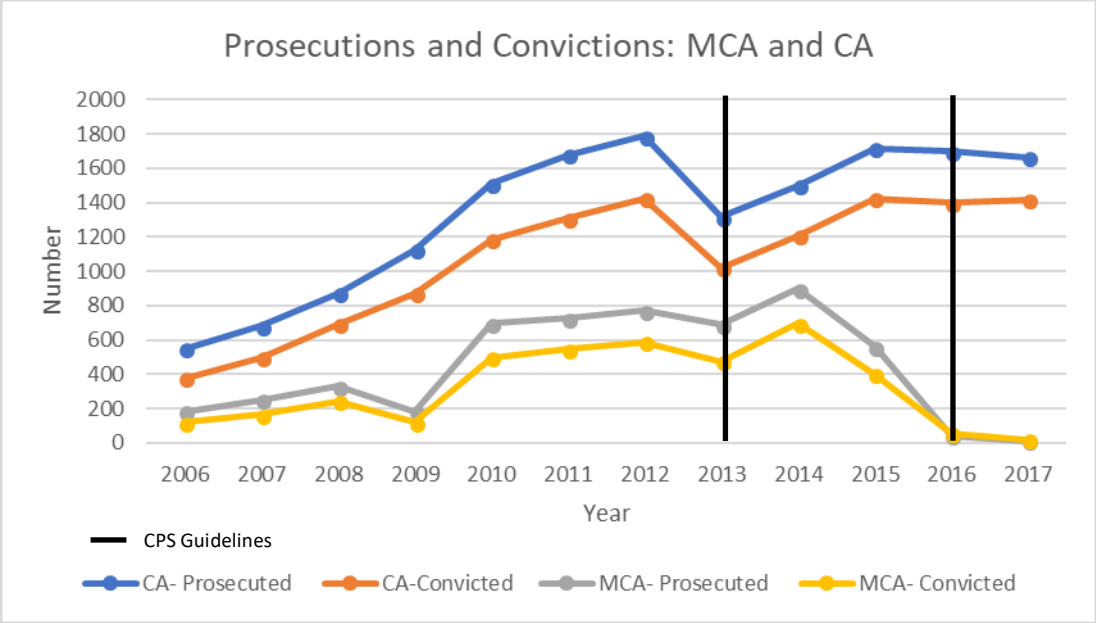
Consequently, the high threshold test placed on social media offences means that victims of online abuse are often left frustrated at the lack of options available to them. For instance, Katie Price an ex-glamour model and well-known celebrity personality has successfully led a campaign calling for a change in the law surrounding abusive comments online.[143] Ms Price has a disabled son Harvey who has been subjected to racist abuse online for several years. She has been very critical of the criminal justice systems approach to the abuse her son has suffered after police dropped charges against two Internet trolls who continued to make abusive comments about Harvey.[144]

The purpose of the guidelines was to create consistency across the criminal justice system when it came to the reporting and prosecution of social media offences. Yet as discussed above mistakes are continuing to be made. For example, in the case of *Chabloz* the original decision by the criminal justice system was not to prosecute. Despite this, Chabloz was later found guilty of three counts under section 127(1) of the Communications Act following an initial private prosecution.[145] Furthermore, since the creation of the social media guidelines the number of prosecutions and convictions under the Malicious Communications Act and section 127 of the Communications Act

[143] Petitions Committee, *Oral evidence: Online abuse and the experience of disabled people* (HC 2017, 759)
[144] Caroline Davies, 'Katie Price urges MPs to act after "horrific" online abuse of son' *The Guardian* (London, 6 February 2018) <https://www.theguardian.com/media/2018/feb/06/katie-price-urges-mps-to-make-online-abuse-a-criminal-offence> accessed 1 May 2018
[145] As upheld by the Crown Court. See *Alison Chabloz* n.126

has decreased, with the exception of the Malicious Communications Act in 2014, as demonstrated in figure six.

Figure 6: *The Number of Prosecutions and Convictions under the Malicious Communications Act and the Communications Act between 2006 and 2017.*[146]



In 2012, 1,787 individuals were prosecuted for offences contrary to section 127 of the Communications Act. By 2013 this figure had dropped to 1,315. Similarly, during the same period prosecutions under the Malicious Communications Act decreased from 772 to 689. By 2017 only 12 prosecutions were brought under the Malicious Communications Act. Likewise, following the guidelines being updated in 2016, a drop in prosecutions and convictions occurred under section 127 of the Communications Act. The social media guidelines were created to ensure consistency across the criminal justice system in England and Wales, not to reduce the likelihood of prosecution. This is further reflected in the Law

[146] Ministry of Justice, 'Criminal Justice System statistics quarterly: December 2017' (*Gov.uk*, 17 May 2018) <https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2017> accessed 25 February 2019

Commission's report into social media offences where they highlight 'controversy over charging and prosecution decisions …'.[147]

Nonetheless, for Rowbottom:

> '[t]he legal responses can, however, seem heavy-handed for what might have been a statement made with little thought while the speaker was sat at a desk at home. Words typed in seconds followed by hitting the enter key can lead to a criminal record or costly civil litigation.'[148]

Indeed, section 127 of the Communications Act and the Malicious Communications Act can be considered wide enough that it would criminalise racist remarks made between two individuals over the telephone.[149] However, it is important to note the serious effects online abuse can have on another, both physically and mentally.[150]

Chapter Overview

Despite the Malicious Communications Act and section 127 of the Communications Act prohibiting online abuse, these legal provisions are insufficient in combatting this growing behaviour. Both provisions govern different types of behaviours which can be conducted online. Despite this these Acts are mainly used to govern grossly offensive messages.[151] Yet the high threshold test associated with grossly offensive communications, though

[147] Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018) [5.73]
[148] Rowbottom n.6, 356
[149] *Director Public Prosecutions v Collins* n.48, per Lord Brown [26-27]
[150] For an in-depth discussion on the effects of online abuse see chapter one.
[151] The Crown Prosecution Service n.87

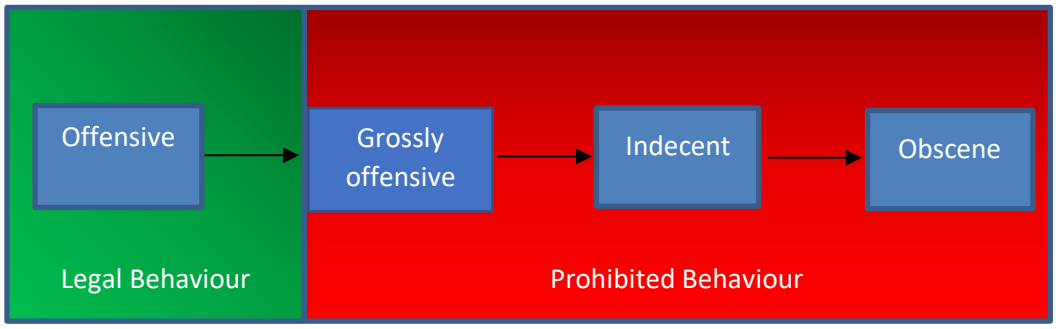
protecting freedom of expression, means victims are often being let down by the criminal justice system.[152]

From the discussion above, it can be seen that a spectrum has been created within the criminal justice system when it comes to inappropriate communications, as illustrated in figure seven. Though issues arise with regards to the boundaries between these types of behaviours. For instance, offensive comments are beyond the scope of the law, but grossly offensive commentary is not. Yet there is no clear distinction in law as to when offensive conduct will be deemed grossly offensive:

> 'Or, to put the matter more pertinently, if the two cases of Woods [the person who sent grossly offensive messages relating to the missing school girl, April Jones] and Thomas [the footballer who sent a homophobic tweet about the divers Tom Daley and Peter Waterfield] are on either side of a line between comments which are merely offensive and those which are grossly so, the question arises as to where that line lies.'[153]

This, in turn has a direct effect on the principle of legality.

Figure 7*: The boundaries between inappropriate and unlawful behaviour online.*



[152] Sandra Laville, 'Online abuse: "existing laws too fragmented and don't serve victims"' *The Guardian* (London, 4 March 2016) <https://www.theguardian.com/uk-news/2016/mar/04/online-abuse-existing-laws-too-fragmented-and-dont-serve-victims-says-police-chief> accessed 1 May 2018
[153] Bliss n.116, 177

As discussed in chapter two the law must be certain, clear and accessible to uphold the principle of legality in the criminal law. The Malicious Communications Act and section 127 of the Communications Act, lacks clarity in terms of what constitutes a grossly offensive communication, which in turn leaves individuals at a disadvantage. In recent years various individuals in the public domain have been vocal about the abuse they and their families have received online, with many of these instances not passing the high threshold test contained in the criminal justice system. Indeed:

> 'The confusion in the case law would seem to demonstrate that emphasising the importance of context in the CPS guidelines may still not be sufficient to guide decisions to charge and prosecute.' [154]

Arguably, the law has 'tilted' too far in the direction of freedom of expression.[155] Those who are subjected to prolonged abuse online are not being adequately protected by the law, meaning other human rights are being breached. How the criminal justice system is attempting to balance inappropriate conduct aided by social media and human rights will be examined in the following chapter.

Chapter Six: Recommendations

- Include a clear and precise definition of false communications with the aid of case law examples;
- Define grossly offensive and menacing material with the aid of case law examples and the CPS guidelines on social media prosecutions; and

[154] Law Commission n.147, [5.76]
[155] Zia Akhtar, 'Malicious communications, media platforms and legal sanctions' (2014) 20(6) Computer and Telecommunications Law Review 179, 181

- Ensure the social media prosecuting guidelines are updated to include examples to illustrate when a comment or conduct goes beyond someone's right to freedom of expression.

Chapter Seven

Freedom of Expression and Social Media

> 'As computers become less expensive, simpler to use and consequently more common in … homes (and workplaces), as the barriers to disseminating information through computers fall, bigots of all kinds are rushing to use the power of modern technology to spread propaganda.'[1]

The use of modern technology has changed how individuals communicate across the globe. Messages can be sent in an instance and those intended to only reach a few reaching thousands within a matter of minutes.[2] With easy access to the online world, online abuse is becoming an increasing problem for jurisdictions across the world.[3] Social media has essentially turned private individuals into 'publishers, content creators and news sources'.[4] With an increase in social media use, law enforcement is attempting to balance Article 10 of the European Convention on Human Rights and Fundamental Freedoms, against other protected rights.

The discussion below will examine freedom of expression in a social media context. To do this, first the definition of freedom of expression will be outlined, before turning to look in detail at Article 10 of the European Convention on Human Rights and Fundamental Freedoms (the Convention).

---

[1] James Banks, 'Regulating hate speech online' (2010) 24(3) International Review of Law Computers & Technology 233

[2] Ed Pilkington, 'Justine Sacco, PR executive fired over racist tweet, "ashamed"' *The Guardian* (London, 22 December 2013) <https://www.theguardian.com/world/2013/dec/22/pr-exec-fired-racist-tweet-aids-africa-apology> accessed 5 October 2018

[3] Daniel Boffey, 'EU threatens to crack down on Facebook over hate speech' *The Guardian* (London, 11 April 2018) <https://www.theguardian.com/technology/2018/apr/11/eu-heavy-sanctions-online-hate-speech-facebook-scandal> accessed 4 September 2018

[4] Anita Bernstein, 'Abuse and Harassment Diminish Free Speech' (2014) 35 Pace Law Review 1, 8

Following on from this, how a person's right to free speech is applied in the context of hate speech and offensive commentary online will be explored before turning to examine privacy in a digital age.

Freedom of Expression

The concept of free speech is considered a fundamental principle of any democratic society. It allows individuals to challenge state authorities, whilst also promoting change within a jurisdiction. It is considered a right that every human should have with States having an obligation to 'respect, protect and promote freedom of opinion and expression.'[5] In 1948 the Universal Declaration of Human Rights (UDHR) was adopted by the United Nations General Assembly to create a unilateral understanding of all aspects of Human Rights, with article 19 of the UDHR protecting a person's right to freedom of expression:

> '(1) Everyone shall have the right to hold opinions without interference. (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.'

Despite this the growing use of the Internet has blurred the lines between freedom of speech and private information. This has led to law enforcement struggling to appreciate when a comment made by an individual online goes beyond the protection of a person's right to free speech.[6]

[5] Council of the European Union, 'EU Guidelines: Freedom of Expression Online and Offline' (*Europa*, 13 May 2014) 3 <https://ec.europa.eu/digital-single-market/en/news/eu-human-rights-guidelines-freedom-expression-online-and-offline>

[6] Alan Sears, 'Protecting Freedom of Expression over the Internet: An International Approach' (2015) 5(1) Notre Dame Journal of International & Comparative Law 171, 172

The right to freedom of expression is protected under several legal provisions worldwide, including, though not limited to, Article 19 of the UDHR, Article 19 of the International Covenant on Civil and Political Rights and Article 10 of the Convention. The United Kingdom is a signatory to these legal provisions and is bound to adhere to the protection of freedom of expression. Below, Article 10 of the Convention will be examined, as the Convention is now part of UK law following the implementation of the Human Rights Act 1998.[7]

Article 10: Freedom of Expression

The European Convention on Human Rights and Fundamental Freedoms came into force on 21 January 1959 and was signed by all 47 Member States of the European Council. The Convention itself consists of several Articles protecting what are considered basic human rights, including the prohibition of torture, the right to life and freedom of expression. Under Article 10 all citizens based in a signatory state are entitled to free speech:

> 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers …'.[8]

In essence, every citizen has the right to express an opinion or thought with the European Court of Human Rights upholding the ideal that even offensive commentary falls within a person's right to freedom of expression.[9] However,

[7] Prior to the Human Rights Act 1998 coming into force, the Convention only applied to the Government.
[8] The European Convention on Human Rights and Fundamental Freedoms Article 10(1)
[9] *Handyside v United Kingdom* (1976) 1 EHRR 737 [49]

the right to free speech is not an absolute right and can be restricted in certain circumstances.

The Articles contained under the Convention can be split into three distinct categories: absolute, limited and qualified. Absolute rights are considered those basic human rights which the State cannot infringe under any circumstance. So, for instance the prohibition of torture is an absolute right, which cannot be breached even in times of national emergency or during times of war.[10] Whereas Article 5, right to liberty, is a limited right whereby it can be restricted under the exceptions contained within the Article itself. For instance, an individual can be deprived of their liberty when detained following a court conviction.[11] The right to freedom of expression is a qualified right:

> 'A public authority can sometimes interfere with your rights if it's in the interest of the wider community or to protect other people's rights. These rights are qualified. Qualified rights may need to be balanced against other people's rights or the rights of the wider community to achieve a fair outcome.'[12]

All qualified rights can be restricted when three criterions are met: the restriction is prescribed by law, the restriction fulfils at least one of the legitimate aims contained in the second paragraph of the Article, and the restriction can be considered as necessary in a democratic society.

[10] The European Convention on Human Rights and Fundamental Freedoms Article 15(2)
[11] The European Convention on Human Rights and Fundamental Freedoms Rights Article 5(1) a
[12] Citizens Advice, 'When can a public authority interfere with your human rights?' (*Citizens Advice*, 2018) <https://www.citizensadvice.org.uk/law-and-courts/civil-rights/human-rights/when-can-a-public-authority-interfere-with-your-human-rights/> accessed 5 September 2018

In England and Wales several laws exist to prohibit certain types of speech. For example, section 127(1) of the Communications Act 2003 prohibits the sending of messages which can be considered as grossly offensive, indecent or obscene, as discussed in detail in chapter six.[13] Nonetheless, the European Court of Human Rights has made it clear that the legal rule prohibiting free speech must be clear and certain as affirmed in *Sunday Times v United Kingdom*:[14]

> 'In the Court's opinion, the following are two of the requirements that flow from the expression "prescribed by law". Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.'[15]

In this matter, the European Court of Human Rights was asked to consider if a tabloid newspapers right to free speech had been infringed after the Attorney General sought, and was granted an injunction preventing articles from being published on the grounds of Contempt of Court.[16] The Sunday Times had run several articles detailing an ongoing legal dispute between users of the pharmaceutical drug Thalidomide, and the manufacturer of the drug Distillers. In the late 1950s and early 1960s Thalidomide had been prescribed to pregnant women for morning sickness. However, the side

[13] Communications Act 2003 section 127(1)
[14] *Sunday Times v United Kingdom* (1979) 2 EHRR 245
[15] *Ibid.,* [49]
[16] 'Contempt of court is the established, if unfortunate, name given to the species of wrongful conduct which consists of interference with the administration of justice. It is an essential adjunct of the rule of law. Interference with the administration of justice can take many forms.' *Attorney General v Punch Ltd and Another* [2002] UKHL 50, [2003] 1 A.C. 1046 per Lord Nicholls of Birkenhead [2]

effects of the drug resulted in women who had taken the medication giving birth to deformed children.

The newspaper articles which were published by the Sunday Times included arguments that Distillers should not amount a legal defence to the allegations against them, along with suggesting some of the evidence that may be presented before the court. Consequently, the Attorney General was granted an injunction for fear that the reports may affect the outcome of the Distillers trial, under the common law of Contempt of Court. The Sunday Times challenged the decision before the European Court of Human Rights on the grounds that the injunction breached their right to freedom of expression. For the European Court of Human Rights, free speech could be limited to maintain the authority of the judiciary, however the law limiting Article 10 had to be sufficiently clear and precise. As a result, the Court concluded that the common law of Contempt of Court was not sufficiently clear, breaching the applicants right to free speech.[17]

The Sunday Times case confirms the key principle of legality in the criminal justice system. Here the law needs to be sufficiently clear and accessible in order to restrict a qualified right. If the law can be considered vague, the restriction will not be upheld by the European Court of Human Rights. As discussed in detail in the previous chapters several laws in England and Wales govern conduct carried out online. Nonetheless, not all these laws can

[17] The decision of the European Court of Human Rights paved the way for the creation of the Contempt of Court Act 1981.

be considered as clear and accessible to adhere to the principle of legality. For example, issues arise in relation to the term 'grossly offensive' contained in section 127(1) of the Communications Act. In fact, as discussed further in the following chapter, in India section 66a of the Information Technology Act 2000 was struck down by the Supreme Court of India, as the term 'grossly offensive' was considered not to conform with the principle of legality.[18]

If the law restricting a person's right to freedom of expression can be considered as clear and accessible, next it must be established that the restriction meets one of the legitimate aims contained within the second paragraph of the Article. Each qualified right within the Convention contains a list of situations whereby a right can be restricted, so long as it fulfils one of the legitimate aims. The legitimate aims differ depending on the right being reviewed. For a restriction on freedom of expression to be upheld it must fulfil one of the following situations:

> '… in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.'[19]

All restrictions on freedom of expression must pursue one of the aims above, failure to comply with the principle will render the restriction unlawful.[20] However to pursue one of the legitimate aims, it needs to be necessary in a democratic society.

[18] For further discussions on India and the Information Technology Act see chapter eight.
[19] The European Convention on Human Rights and Fundamental Freedoms Article 10(2)
[20] *Handyside* n.9, [49]

For a restriction to be considered as necessary in a democratic society, it is for the courts to establish:

> '… whether: (i) the legislative objective is sufficiently important to justify limiting a fundamental right; (ii) the measures designed to meet the legislative objective are rationally connected to it; and (iii) the means used to impair the right or freedom are no more than is necessary to accomplish the objective.'[21]

The concept of 'necessary in a democratic society' was explored in detail in *Dudgeon v United Kingdom.*[22] *Dudgeon* concerned the lawfulness of a legal provision contained in the law of Northern Ireland which criminalised homosexuality. For the applicant who sought leave before the European Court of Human Rights, the law breached Article 8(1) of the Convention: the right to privacy.

Like Article 10, the right to privacy is a qualified right and can be limited when it is prescribed by law, fulfils one of the legitimate aims contained in the second paragraph of the article, and can also be considered as necessary in a democratic society. For the European Court of Human Rights, the law in question was sufficiently clear and pursued one of the legitimate aims contained under Article 8(2). Nevertheless, issues arose in relation to the restriction being necessary in a democratic society:

> 'It cannot be maintained in these circumstances that there is a "pressing social need" to make such acts criminal offences, there being no sufficient justification provided by the risk of harm to vulnerable sections of society requiring protection or by the effects on the public. On the issue of proportionality, the Court considers that such justifications as there are for retaining the law in force unamended are outweighed by the detrimental effects which the very existence of the legislative provisions in question can have on the life of a person of homosexual orientation like the applicant. Although

[21] *de Freitas v Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing* [1999] 1 AC 69 (PC) 80
[22] *Dudgeon v United Kingdom* (1981) 4 EHRR 149

> members of the public who regard homosexuality as immoral may be shocked, offended or disturbed by the commission by others of private homosexual acts, this cannot on its own warrant the application of penal sanctions when it is consenting adults alone who are involved.'[23]

Essentially, it was found that criminalising homosexual acts between two consenting adults was not considered as necessary in a democratic society therefore breaching Article 8 of the Convention.[24] The judgment of the European Court of Human Rights in *Dudgeon* illustrates that if there is more than one way to achieve a legitimate aim, the State has to use the least intrusive method, otherwise the restriction of the Article will be considered unlawful.

In the United Kingdom all public bodies must adhere to the protection of human rights, as governed under the Human Rights Act 1998.[25] Under section 6(3) of the Act, public bodies are defined as '(a) a court or tribunal, and (b) any person certain of whose functions are functions of a public nature …'. Here, the criminal justice system including the courts, are under a legal duty to consider human rights when coming to a decision on a matter before them. For instance, if a person is prosecuted for the sending of menacing communications contrary to section 127(1) of the Communications Act, the court when determining its judgment, must consider all rights contained in the Convention. In cases concerning online abuse, this would include the speakers right to freedom of expression and the victims right to

[23] *Ibid.,* [60]
[24] Later parts of this chapter will examine in detail the right to privacy as guaranteed under Article 8.
[25] Prior to the Human Rights Act 1998, citizens could only invoke their Human Rights before the European Court of Human Rights when the State was in breach of their obligations.

privacy, discussed in more detail in later parts of this chapter. The following sections will outline how freedom of speech is currently applied in matters concerning hate speech and offensive commentary online.

Hate Speech and Freedom of Expression

Hate speech is a growing issue within Western society[26] and is defined in the criminal justice system of England and Wales as:

> '… a range of criminal behaviour[s] where the perpetrator is motivated by hostility or demonstrates hostility towards the victim's disability, race, religion, sexual orientation or transgender identity.'[27]

Following a rise in Internet usage society has witnessed an increase in online hate speech.[28] Though the Convention itself does not contain a 'free-standing' right prohibiting discrimination on grounds of a person's disability, race, or indeed any of the other protected characteristics found in the law of England and Wales.[29]

An individual's right to freedom of expression includes a variety of different forms of communications including, though not limited to, art, radio, books and dance. As outlined above the right to free speech can be limited when three criterions are met: the restriction is prescribed by law, the restriction

---

[26] Caroline Davies, 'One-quarter of Britons witnessed hate speech in past year, poll finds' *The Guardian* (London, 27 January 2018) <https://www.theguardian.com/society/2018/jan/27/uk-hate-speech-poll-holocaust-memorial-day-2018> accessed 1 November 2018

[27] The Crown Prosecution Service, 'Hate crime' (*CPS.gov*, 2018) <https://www.cps.gov.uk/hate-crime> accessed 26 September 2018

[28] Rachel Roberts, 'Online hate crime to be tackled by new national police hub, Home Secretary says' *The Independent* (London, 8 October 2017) <https://www.independent.co.uk/news/uk/politics/online-hate-crime-amber-rudd-home-office-national-police-hub-facebook-twitter-trolls-a7988411.html> accessed 5 October 2018

[29] Equality and Human Rights Commission, 'Article 14: Protection from Discrimination' (*Equality Human Rights*, 4 May 2016) <https://www.equalityhumanrights.com/en/human-rights-act/article-14-protection-discrimination> accessed 23 October 2018

pursues one of the legitimate aims contained in the second paragraph of the article, and the restriction can be considered as necessary in a democratic society. In England and Wales hate crime is prohibited under several Acts of Parliament. For instance, under part 3 of the Public Order Act 1986 expressions of racial hatred are prohibited.[30] In addition, the restriction of hate speech can be considered as pursuing at least one of the legitimate aims contained in Article 10(2), 'protecting the rights of others.' Here, the State can restrict a person's expressions if it can be considered necessary in a democratic society to ensure the protection of other protected rights contained in the Convention. Affirmed further in Article 17 of the Convention.

Article 17 states:

> 'Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention.'[31]

Put simply, a person cannot rely on the protection of a given Article within the Convention at the detriment of another Article right. So, for example a person cannot spread racial hatred as part of their right to freedom of expression if it is considered to significantly affect other rights contained in the Convention. For instance, Article 8 the right to privacy, as demonstrated in *Glimmerven en Hagenbeek v Netherlands.*[32]

[30] For a discussion on the issues relating to the use of the Public Order Act 1986 in a social media context see chapter four.
[31] The European Convention on Human Rights and Fundamental Freedoms Article 17(1)
[32] *Glimmerven en Hagenbeek v Netherlands* [1979] ECTHR 8

The European Court of Human Rights was asked to consider if the Netherlands had breached the applicants right to free speech by prohibiting them from distributing leaflets. Glimmerven and Hagenbeek, which had previously been declared as a prohibited organisation under the Civil Code of the Netherlands, had distributed leaflets advocating the removal of 'all Surinamers, Turks and other so-called guest workers from the Netherlands.' Before the court the Dutch Government accepted that they had infringed the applicants right to free speech, however the Government successfully argued that Article 17 prohibited Glimmerven and Hagenbeek from exploiting Article 10 to spread racial hatred:

> 'The Netherlands' authorities in allowing the applicants to proclaim freely and without penalty their ideas would certainly encourage the discrimination prohibited by [these] provisions of the Convention … [such activities being] contrary to the text and spirit of the Convention.'[33]

The arguments put forward by the Dutch Governments legal team were accepted by the European Court of Human Rights, where the court held that the applicants right to freedom of expression was lawfully infringed by the State.

In recent years, the criminal justice system of England and Wales has seen an increase in hate-related offences. Between 2016 and 2017 the police recorded 80,393 offences where it was considered that hate crime was a motivating factor in the offence, this was an increase of 29% on the previous year.[34] In particular, the criminal justice system has witnessed a rise in hate

[33] *Ibid.,* [196]
[34] Home Office, 'Statistical News Release: Hate Crime, England and Wales, 2016/17' (*Gov.uk*, 17 October 2017)

speech online,[35] calling for the Crown Prosecution Service (CPS) to announce a 'crackdown' on social media hate crime:

> 'When an ever-greater amount of our time is spent online, it is only right that we [criminal justice system] do everything possible to ensure that people are protected from abuse that can now follow them everywhere via the screen of their smartphone or tablet. Whether shouted in their face on the street, daubed on a wall or tweeted into their living room, hateful abuse can have a devastating impact on victims.'[36]

Significant weight is given to online abuse which targets one of the protected characteristics associated with hate crime. Yet this is not necessarily reflected in the CPS guidelines on social media prosecutions.

As examined in detail in the previous chapter, the CPS in 2013 released guidelines on social media prosecutions following concerns that there was a lack of consistency across police forces. The guidelines were later updated in 2016 and 2018 to reflect, amongst other things, the link between social media related offences and hate crime. The guidelines uphold the idea that in order for the law to intervene with conduct carried out on social media, a high evidential and public interest threshold will need to be passed, even in matters related to hate speech:

> 'The high threshold at the evidential stage and the public interest and [European Convention on Human Rights] considerations … apply to social media communications offence hate crime cases, as they do to other cases.'[37]

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651851/hate-crime-1617-hosb1717snr.pdf> accessed 26 September 2018

[35] Alison Saunders, 'Hate is hate. Online abusers must be dealt with harshly' *The Guardian* (London, 21 August 2017) <https://www.theguardian.com/commentisfree/2017/aug/20/hate-crimes-online-abusers-prosecutors-serious-crackdown-internet-face-to-face> accessed 26 September 2018

[36] *Ibid.,*

[37] The Crown Prosecution Service, 'Guidelines on Prosecuting Cases Involving Communications Sent via Social Media' (*CPS.gov*, 21 August 2018) [54]

Subsequently, communications which can be considered as containing a hate crime element will not automatically invoke the criminal law, instead prosecutors are encouraged to consider the contextual element behind the communication:

> 'When assessing communications that appear to be motivated by such discrimination or demonstrate such hostility, prosecutors should be alert to any additional reference or context to the communication in question. Such references or context may sometimes elevate a communication that would otherwise not meet the high threshold to one that, in all the circumstances, can be considered grossly offensive. For instance, a reference within the communication to a recent tragic event, involving many deaths of persons who share any of the protected characteristics.'[38]

Despite the initial stance by the CPS in relation to tackling hate speech online, this has not been reflected in the social media prosecuting guidelines. Consequently, issues have arisen whereby the police and the CPS have neglected to identify when a person's communications go beyond their right to freedom of expression.[39] This is evidently true when the complained about behaviour falls outside the definition of a hate crime and instead can be labelled as offensive commentary.

Offensive Comments and Freedom of Expression

The following discussion will examine how the courts balance a person's right to freedom of expression against comments which can be defined as offensive or abusive. As explored in detail in chapter one online abuse is on

<https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media> accessed 26 September 2018

[38] *Ibid.,* [55]

[39] *R v Alison Chabloz* Westminsters' Magistrates Court 25 May 2018 (unreported)

the increase.[40] Consequently, there has been a rise in reports made to the police in relation to abuse conducted online.[41] Here, the criminal justice system has to distinguish between comments which can be considered as merely offensive, and therefore protected under Article 10, against comments which go beyond free speech to warrant criminal law intervention.

From the discussions above, a person's right to freedom of expression includes a variety of different modes of communications. In fact, the European Court of Human Rights has upheld that freedom of expression, includes the right to be offensive as governed by *Handyside v UK.*[42] Richard Handyside was prosecuted and convicted under the Obscene Publications Act 1959 and 1964, for the distribution of 'The Little Red School Book'. The book which was written by two Danish school teachers was published in 1969 and contained several pages on sex, drugs and alcohol. Following his conviction and subsequent failed appeals in the judicial system in England and Wales, Handyside lodged an application before the European Court of Human Rights claiming his right to freedom of expression had been breached.

Though Handyside's application was unsuccessful, with the European Court of Human Rights concluding that the restriction did not breach Article 10 of

[40] The BBC, 'Teenager's life "ruined" by Live.me and Twitter "trolls"' *The BBC* (London, 24 October 2017) <http://www.bbc.co.uk/news/uk-england-41693437> accessed 30 January 2018
[41] *Ibid.,*
[42] *Handyside* n.9

the Convention, the judges supported the concept that offensive speech should be protected:

> 'Freedom of expression constitutes one of the essential foundations of such a society, one of the basic conditions for its progress and for the development of every man. Subject to Article 10 (2), it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population.'[43]

The European Court of Human Rights maintains that an individual has the right to offend another without interference from the state, a concept that is supported by cyber-libertarians.

Cyber-libertarianism:

> 'refers to a perspective (some would say philosophy) which claims that cyberspace and the Internet should be regarded as uncontrolled and unregulated electronic spaces where anyone is free to be whatever they wish and express themselves however they like.'[44]

In essence, for cyber-libertarians 'earthbound' laws should not apply to cyberspace.[45] Dyson, Gilder, Keyworth and Toffler argue that the emergence of new technology, such as that of the Internet, has created an 'Information Superhighway' which should be for the benefit of its users, and consequently beyond the reach of the law.[46] They go as far as arguing that even computer hacking is for the benefit of 'economic growth and trade leadership'.[47] Similarly, Johnson and Post suggest that if the Internet is to be regulated,

---

[43] *Ibid.,* [49]
[44] David J. Bell, Brian D Loader, Nicholas Pleace & Douglas Schuler, *Cyberculture: The Key Concepts* (Routledge 2004) 35
[45] Paul Bernal, *The Internet, Warts and All: Free Speech, Privacy and Truth* (Cambridge University Press 2018) 20
[46] Esther Dyson, George Gilder, George Keyworth & Alvin Toffler, 'Cyberspace and the American Dream: A Magna Carta for the Knowledge Age' (1994) Future Insight <http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html> accessed 26 September 2018
[47] *Ibid.,*

provisions need to be independent and separate from the 'material world'.[48] Here, for cyber-libertarians, technology in particular the Internet, should be beyond the reach of government control and regulation. This theoretical perspective has gained momentum within some Internet based organisations. For instance, Wikipedia founder Jimmy Wales has been vocal about the Internet being beyond the realms of State intervention.[49]

Regardless of the approach endorsed by cyber-libertarians, it has come to be accepted that the Internet now represents parts of modern life, which does not have a separate identity to 'real-life',[50] or as potently put by Bernal, '[t]he Internet is now integral to the way society operates.'[51] For Bernal:

> '[c]onversely, some of the activities that have developed on the Internet, from the distribution of child abuse imagery to networks of extremist material, cyberbullying, hate speech and much more - make it impossible for governments not to become involved. If the Internet is riven with lawlessness, so is our society; the two cannot be treated separately.'[52]

Most notably, Reed argues that whilst a physical body remains in a place controlled by a Government, the law will have to intervene.[53] Here, the law should govern individuals online conduct but not at the expense of freedom of expression. As explored in chapter one the Internet now dominates much of society. Its use has changed political discourse, changed how businesses

[48] David Johnson & David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367
[49] David Golumbia, 'Cyberlibertarianism: The Extremist Foundations of "Digital Freedom"' (Clemson University, South Carolina, September 2013)
[50] Barry Wellman & Caroline Haythornthwaite (eds), *The Internet in Everyday Life* (John Wiley & Sons 2008) 25
[51] Bernal n.45, 19
[52] *Ibid.,* 21
[53] Chris Reed, *Internet Law: Text and Materials* (Cambridge University Press 2004) 174-175

operate and has changed how society communicates. It is clear that the Internet cannot be considered as a separate entity from that of 'real-life'.

From the jurisprudence of both the European Court of Human Rights and the courts of the UK, it is clear that different types of speech incur different types of protection under the law:

> 'There are undoubtedly different types of speech, just as there are different types of private information, some of which are more deserving of protection in a democratic society than others. Top of the list is political speech. The free exchange of information and ideas on matters relevant to the organisation of the economic, social and political life of the country is crucial to any democracy. Without this, it can scarcely be called a democracy at all.'[54]

Whereas political speech is given the highest form of protection, speech which can be labelled as mere gossip is not necessarily shielded from the law.[55]

Despite low-level speech being given some protection, the jurisprudence of the courts and human right bodies indicate that the criminal justice system will 'tilt' in the direction of freedom of expression.[56] In June 2011 the Special Rapporteur, along with other human right agencies issued a Joint Declaration supporting freedom of expression in a digital age.[57] Emphasis was placed on the idea that free speech online needs to be protected from significant government interference, even in times of public safety and national security. The declaration upholds that all citizens should have

---

[54] *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 A.C. 457 per Lady Baroness-Hale [148]
[55] Jacob Rowbottom, 'To rant, vent and converse: protecting low level digital speech' (2012) 71(2) Cambridge Law Review 355, 357
[56] Zia Akhar, 'Malicious communications, media platforms and legal sanctions' (2014) 20(6) Computer and Telecommunications Law Review 179, 181
[57] Laura Scaife, *Handbook of Social Media and the Law* (Routledge 2015) 36

universal access to the Internet, a concept which has been supported by the European Court of Human Rights:

> '[The Internet is] one of the principal means by which individuals exercise their right to freedom of expression and information providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest.'[58]

The significant protection of free speech, even speech which can be labelled as offensive has been supported further by the United Nations. In the United Nations Comprehensive Study on Cybercrime they argue that the restriction of speech which can be considered as defamatory, obscene or insulting may not warrant criminal law intervention.[59] Indeed, in matters concerning hate-related speech and offensive commentary the justice system needs to consider:

> '(i) the context of the statement; (ii) the position or status of the speaker; (iii) the intent (negligence and recklessness should not suffice); (iv) the content or form of statement; (v) the extent of the statement; and (vi) the degree of risk of resulting harm.'[60]

Consequently, for the United Nations there needs to be a '… genuine and serious incitement to extremism, as opposed to ideas that simply offend, shock or disturb others'[61] in order to restrict freedom of expression. Though little consideration is given to the effects of becoming a victim of online abuse and a person's right to privacy, discussed further in the following section.

Online Abuse and the Right to Privacy

For Bernal:

---

[58] *Yildirim v Turkey* App no 3111/10 ECTHR 2012-VI [52-54]
[59] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime- Draft* (United Nations, February 2013) 116
[60] *Ibid.,* 112
[61] Scaife n.57, 42

> '[t]he problem with the Internet is that the boundaries between what is public and what is private have been more than just blurred; they have been all but obliterated.'[62]

In fact, social media sites such as Facebook actively encourage users to distribute private information, for instance birthdays and general interests.[63] Consequently, the expansion of the Internet has distorted the lines between what is considered the public and private domain, clearly illustrated following the launch of the Samaritans Rader App.[64]

In 2014 the Samaritans, a UK based mental health charity, released an App[65] aimed at reducing suicide. The App once downloaded onto the user's smart device would link to an individual's Twitter profile to scan tweets in the user's homepage. Using a list of predetermined keywords, the App would then point out if someone who they 'followed' on Twitter indicated possible suicidal tendencies, even if the other user did not have access to the App. Following its launch, the Samaritans came under heavy criticism for breaching Twitter user's privacy. The original stance taken by the Samaritans was to justify the App's usage by arguing that comments made on Twitter were in the public domain, and as a result there was no expectation of privacy. Two months after the App was launched, the Samaritans suspended its usage.[66]

---

[62] Bernal n.45, 18
[63] Lauren Gelman, 'Privacy, Free Speech, and "Blurry Edged" Social Networks' (2009) 50(5) Boston Collage Law Review 1315, 1328
[64] Bernal n.45, 146-149.
[65] 'Apps [are] short applications, an app is software, for use on a desktop, laptop, tablet or smartphone, that allows the user to apply the power of system software for a particular purpose.' Jeremy Harris Lipschultz, *Social Media Communication: Concepts, Practices, Data, Law and Ethics* (Routledge 2018) 345
[66] Samaritans, 'Samaritans Rader' (*Samaritans*, 10 March 2015) <https://www.samaritans.org/how-we-can-help-you/supporting-someone-online/samaritans-radar> accessed 26 October 2018

The distinction between private and public information on the Internet continues to be a contentious issue though academics such as Bernal[67] and Gelman,[68] maintain that privacy does exist online. The balancing of Article 8 the right to privacy, and Article 10 freedom of expression, is not unique to the digital age. Much of the jurisprudence relating to these two rights stems from traditional forms of media such as the press.[69] Under Article 8 of the Convention '[e]veryone has the right to respect for his private and family life, his home and his correspondence.' As discussed earlier, like that of freedom of expression, the right to privacy is a qualified right and can be restricted when prohibited by law, necessary in a democratic society, and fulfils one or more of the following legitimate aims:

> '… in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'[70]

In matters concerning social media the criminal justice system tilts in the direction of freedom of expression. For instance, as discussed in chapter six the CPS guidelines on social media prosecutions makes significant mention of free speech with little reference given to privacy. For Woods, the criminal justice systems approach to using Article 10 as opposed to Article 8 when concluding if a comment invokes the criminal law is a flaw in itself.[71] Article

---

[67] Bernal n.45, 16
[68] Gelman n.63
[69] Lorna Woods, 'Social Media: it is not just about Article 10' in David Mangan & Lorna E. Gillies (eds), *The Legal Challenges of Social Media* (Edward Elgar Publishing 2017) 109. For Bernal, the use of traditional media law is not necessarily suitable for social media. See, Paul Bernal, *The Internet, Warts and All: Free Speech, Privacy and Truth* (Cambridge University Press 2018) 25
[70] The European Convention on Human Rights and Fundamental Freedoms Article 8(2)
[71] Woods n.69, 105

10 the right to free speech, is not fully concerned with human interaction unlike that of Article 8. Consequently, Article 10 can be considered too broad. Here, the European Court of Human Rights has given a significantly wide definition of freedom of expression and does not always fully appreciate the importance of Article 8.[72] Whereas Article 8 is 'deeply contextual'.[73]

The competing interests contained in both Article 8 and Article 10 has imposed a balancing act within the courts. In *Campbell v MGN Limited*,[74] the House of Lords had to directly address the issue of freedom of expression versus the right to privacy:

> 'The present case concerns one aspect of invasion of privacy: wrongful disclosure of private information. The case involves the familiar competition between freedom of expression and respect for an individual's privacy. Both are vitally important rights. Neither has precedence over the other. The importance of freedom of expression has been stressed often and eloquently, the importance of privacy less so. But it, too, lies at the heart of liberty in a modern state. A proper degree of privacy is essential for the well-being and development of an individual. And restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.'[75]

On 1 November 2001 The Mirror a newspaper tabloid based in the United Kingdom ran a story exposing that Naomi Campbell a well-known supermodel, was seeking help for alcohol and drug addictions. The story, which was featured on the front page of the paper contained the following headline: 'Therapy: Naomi outside meeting'. The article contained specific information regarding the type of treatment she was receiving, how often she was attending group sessions, and a photograph of Ms Campbell leaving a

[72] *Ibid.,*
[73] *Ibid.,* 117
[74] *Campbell* n.54
[75] *Ibid.,* per Lord Nicholls of Birkenhead [12]

meeting in London. Following the article being published, Ms Campbell sought immediate legal action, stating that MGN limited had committed the equitable doctrine of breach of confidence and in turn, her privacy had been infringed.

The High Court upheld Ms Campbell's claim, coming to the judgment that the actions of MGN limited was unlawful and awarded her £3,500 in damages. This decision was later overturned by the Court of Appeal. Consequently, Ms Campbell appealed the decision before the House of Lords. Here, the House of Lords examined in detail both a person's right to privacy and a person's right to freedom of expression. The Law Lords by a 3:2 majority, came to the opinion that MGN had acted unlawfully by disclosing the details of the treatment Ms Campbell was seeking, and for the publication of the picture which displayed the supermodel leaving a Narcotics Anonymous group.

Though the case above relates to traditional types of media, in this instance tabloid newspapers, the approach undertaken by the Law Lords in coming to their opinion indicates a novel method in the balancing of Article 8 and 10, which has not been mirrored in matters concerning digital media. First, the concept of privacy was examined by the House of Lords. Privacy:

> '… extends to aspects relating to personal identity, such as a person's name or picture, and furthermore includes a person's physical and psychological integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings. There is therefore a zone of interaction with others, even in a public context, which may fall within

the scope of "private life".'[76]

Privacy is more than just the protection of acts conducted in a private setting. It includes the right for a person not to have their physical or psychological integrity infringed. The concept of privacy underpins free speech,[77] complete free speech would limit the speech of the minority,[78] whilst also having significant psychological effects on those subjected to it.

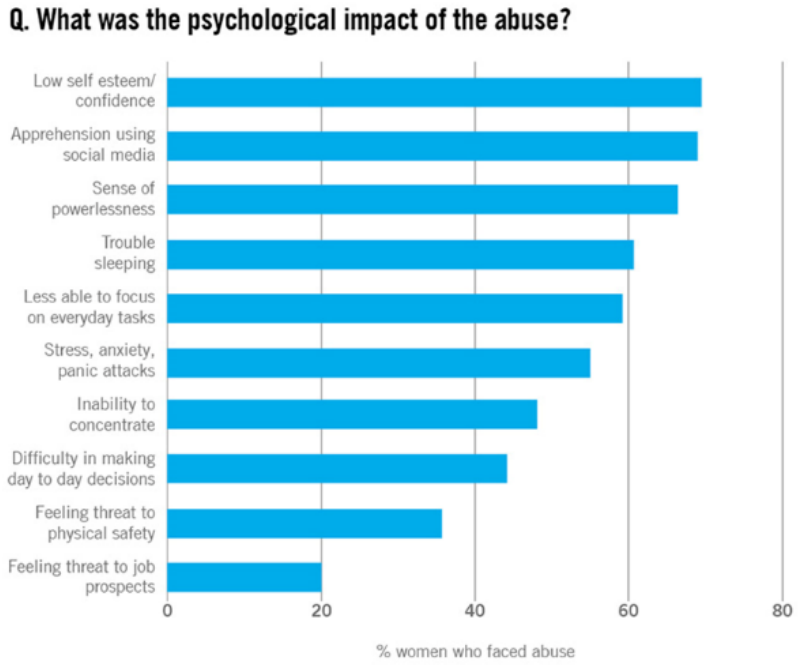
In recent years research has started to emerge examining the effects of online abuse. Research undertaken by Amnesty International found that in the United Kingdom, of those surveyed, 1 in 5 women had experienced abuse online, of these, over half stated that the abuse they experienced was misogynistic.[79] Amnesty International's research went further to expose the underlying effects this type of abuse can have on victims, as shown in figure eight. Of those who took part in the research, 55% of participants in the UK stated that they had experienced anxiety, stress or panic attacks as a result of online abuse;[80] with a further 24% of those surveyed across Denmark, Italy, New Zealand, Poland, Spain, Sweden, the UK and USA feeling that their family's safety was at risk.[81] Similarly in research conducted by Bates, she exposed the underlying psychological effects becoming subjected to revenge pornography can have upon an individual:

---

[76] *Pfeifer v Austria App* no 125561/03 [2007] ECTHR 935 [33]
[77] Bernal n.45, 145
[78] *Ibid.,* 106
[79] Amnesty International UK, 'Online abuse of women widespread in UK' (*Amnesty International*, 2017) <https://www.amnesty.org.uk/online-abuse-women-widespread> accessed 3 October 2018
[80] *Ibid.,*
[81] Amnesty International, 'Amnesty reveals alarming impact of online abuse against women' (*Amnesty International*, 27 November 2017) <https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/> accessed 3 October 2018

'... participants discussed their experiences of trust issues, PTSD [post-traumatic stress disorder], anxiety, depression, loss of control, and how revenge porn affected their self-esteem.'[82]

Figure 8: *The psychological effects on women who experience online abuse in the UK.*[83]



Bates conducted 18 in-depth interviews with women who had been subjected to revenge pornography. In these interviews participants spoke openly about the psychological effects this behaviour had on them:

'When the actual video was released, um, well, I can admit now that I was suicidal, and … to let you know how suicidal I was, I didn't tell anybody because I knew if I told anyone that I just wanted to kill myself that they would try to stop me, so I didn't tell anyone because I didn't [*sic*] want anyone to stop me.'[84]

Like that of the research undertaken by Amnesty International, Bates exposes the real-life implications becoming subjected to online abuse can have on a person. Recently a study conducted by John *et al* found that those

[82] Samantha Bates, 'Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors' (2017) 12(1) Feminist Criminology 22, 38
[83] Amnesty International n.81
[84] Bates n.82, 32

aged under 25, were 2.3 times more likely to self-harm or display suicidal tendencies as a consequence of cyberbullying.[85] If privacy includes the right not to be subjected to physical or psychological harm, then the overall effects of online abuse need to be taken into consideration by the criminal justice system.

Cases which have recently come before the criminal justice system, concerning social media, consider in detail freedom of expression, with little emphasis placed on privacy. In *Campbell* the Law Lords examined Ms Campbells right to privacy first, before looking at freedom of expression:

> '… [The] question is whether the objective of the restriction on the article 10 right - the protection of [Ms] Campbell's right under article 8 to respect for her private life - is sufficiently important to justify limiting the fundamental right to freedom of expression …'.[86]

Here, the justice system should focus on the infringement of the victims right to privacy, before turning to examine freedom of expression. Though freedom of expression is important to maintain a democracy, this should not be at the detriment of another person's mental health. Online abuse can have significant effects on a person's wellbeing and in some instances has resulted in victims taking their own life.[87]

---

[85] Ann John *et al*, 'Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review' (2018) 20 (4) Journal of Medical Internet Research 129. See also, Sarah Knapton, 'Cyberbullying makes young people twice as likely to self harm or attempt suicide' *The Telegraph* (London, 22 April 2018) <https://www.telegraph.co.uk/science/2018/04/22/cyberbullying-makes-young-people-twice-likely-self-harm-attempt/> accessed 10 October 2018

[86] *Campbell* n.54, per Lord Hope of Craighead [113]

[87] Will Worley, 'Mother of cyber bullying victim pens heartbreaking open letter in response to his suicide' *The Independent* (London, 6 October 2016) <https://www.independent.co.uk/news/uk/home-news/mother-open-letter-cyber-bullying-victim-suicide-online-social-media-a7347531.html> accessed 4 October 2018. See also, Knapton n.85

It is not only the psychological effects of online abuse that can affect a person's right to privacy. Berstein argues that abuse and harassment online can lead a person to withdraw from social media, which in turn has an effect on a person's right to privacy, along with freedom of expression.[88] To exclude oneself from the Internet is to put yourself at a disadvantage, as the Internet allows individuals to challenge another's view, whilst also promoting change within society.[89]

For the United Nations, the use of the Internet is considered a right that every human being should have: 'The Special Rapporteur calls upon all States to ensure that Internet access is maintained at all times, including during times of political unrest.'[90] Online abuse limits this right as victims are often choosing to withdraw from the online world in a bid to regain some control. For example, Sara Payne the mother of Sarah Payne, a schoolgirl murdered in July 2000, chose to close her Twitter account following a campaign of online harassment.[91]

---

[88] Bernstein n.4, 19

[89] For example, in recent years society has witnessed the emergence of social media to challenge societies attitudes to rape, with #BeenRapedNeverReported; campaigns tackling the stigma surrounding domestic violence, with #WhyIStayed; and #GirlsLikeUs used to combat stereotypical attitudes against transwomen. See, Jessamy Gleeson, '"(Not) working 9–5": the consequences of contemporary Australian-based online feminist campaigns as digital labour' (2016) 16(1) Media International Australia 77 <http://journals.sagepub.com/doi/pdf/10.1177/1329878X16664999> accessed 12 August 2019

[90] Frank La Rue, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (*Human Rights Council*, 16 May 2011) [79] <https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf> accessed 3 October 2018

[91] Claire Cohen, 'Twitter trolls: The celebrities who've been driven off social media by abuse' *The Telegraph* (London, 18 November 2014) <https://www.telegraph.co.uk/women/womens-life/11238018/Celebrity-Twitter-trolls-The-famous-people-whove-been-driven-off-social-media-by-abuse.html> accessed 3 October 2018

As mentioned in the discussion above Article 17 of the Convention states:

> 'Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention.'

Consequently, freedom of expression cannot be used as an excuse when it comes to online abuse that has a significant effect on a person's right to privacy, yet the CPS guidelines on social media prosecutions makes very little reference to Article 8 of the Convention. Instead, the guidelines emphasis the need to protect freedom of expression. Though free speech is an important legal principle, it cannot be considered a 'trump' card over that of privacy:

> 'Any restriction of the right to freedom of expression must be subjected to very close scrutiny. But so too must any restriction of the right to respect for private life. Neither Article 8 nor Article 10 has any pre-eminence over the other in the conduct of this exercise. As Resolution 1165 of the Parliamentary Assembly of the Council of Europe (1998), para 11, pointed out, they are neither absolute not in any hierarchical order, since they are of equal value in a democratic society.'[92]

Chapter Overview

The approach undertaken by the criminal justice system indicates that when it comes to online abuse freedom of expression will be of paramount importance. Those who commit abuse online often use the concept of free speech to justify their comments but at the same time use this principle to reduce another's speech. The jurisprudence of the European Court of Human Rights supports the idea that freedom of expression is vital in a

[92] *Campbell* n.54, per Lord Hope of Craighead [115]

democratic society,[93] with individuals having a right to be offensive, reflected in the criminal justice system in England and Wales. Furthermore, the CPS guidelines on social media prosecutions reflect the importance of free speech. Contained within the guidelines themselves is a section specifically looking at Article 10 of the Convention. Here, the CPS supports the idea that free speech will create a high threshold to be passed before the criminal law should intervene with online commentary. Yet little reference is made to Article 8, the right to privacy.

Privacy is more than someone's right to a private life away from the public domain. It concerns an individual's right to both physical and psychological integrity, online abuse breaches both. The effects of becoming subjected to online abuse have been evidenced in numerous reports examining abuse online. In some instances, the effects of becoming subjected to abuse and online trolling have forced individuals off the Internet. In addition, those who have been targeted online have reported suffering from post-traumatic stress disorder, and in some instances have committed suicide due to the continued abuse they experience,[94] all of which infringe upon a person's right to privacy.

Privacy is of paramount importance when it comes to deciding if a person should be prosecuted for their online conduct. Presently, emphasis is placed on ensuring the perpetrators right to freedom of expression is not infringed,

[93] *Handyside* n.9, [49]
[94] Samantha Bates, 'Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors' (2017) 12(1) Feminist Criminology 22

with little reference being made to the victims right to privacy. Here, the criminal justice system should invoke the approach of the House of Lords in *Campbell*, by examining privacy first before turning to look at freedom of expression. This will ensure that the police, the CPS and the courts are considering the full effects of online abuse, before coming to a decision.

Chapter seven: Recommendations

- Update the CPS guidelines on social media prosecutions to ensure privacy is included;
- Ensure better education is given to the police and social media users concerning the psychological effects of online abuse; and
- Digital training for police officers to ensure they fully understand the effects of online abuse on those who are subjected to it.

Chapter Eight

International Perspectives of Social Media and the Law

> 'The open digital spaces they [social media sites] provide must not become breeding grounds for, for instance, terror, illegal hate speech, child abuse or trafficking of human beings, or spaces that escape the rule of law.'[1]

The purpose of this chapter is to explore how other institutions and States use both legislative and non-legislative approaches to govern conduct carried out on social media through the lens of legality. Across the globe there is no one universal approach to tackling unlawful behaviour online, instead States have implemented their own initiatives in an attempt to overcome the growing issues of the digital age. These initiatives range from non-legally binding codes of conduct to specific laws aimed at both the online user and social media companies. The discussion below will outline the methods undertaken by the European Union, Australia, Germany and India in tackling cybercrime. The rationale for focussing on these institutions and States surrounds the different approaches each has taken in tackling illegal online conduct.

The European Union

The concept of the European Union (EU) is built on several principles, including the creation of an Internal Market across all Members of States. The purpose of the Internal Market is '… to promote throughout the Community [EU] a harmonious development of economic activities'[2] built on

[1] Commission, 'Tackling Illegal Content Online: Towards an enhanced responsibility of online platforms' COM (2017) 55 final 2

[2] Originally contained in The Treaty of Rome [1957] Article 2. Similar provisions are made in the Treaty of Lisbon [2007] OJ C-306/1 Article 2

four fundamental freedoms: the free movement of people, the free movement of goods, the free movement of capital and the free movement of services.[3] Since the creation of the EU, States have had to adapt quickly to the changing nature of technology.

To ensure consistency across the EU, directives have been created to help establish the boundaries of 'information society services.'[4] A directive, in its simplest form is 'a legislative act that sets out a goal that all EU countries must achieve.'[5] Each Member of State can choose how they will achieve the goal outlined in a directive through its own legal provisions. Consequently, following a rise in Internet usage and the changing nature of a technology-based age, several directives have been created to govern online conduct,[6] with the EU Commission upholding the idea that what is illegal offline is also illegal online.[7]

In 2000 the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (the

[3] Consolidated versions of the Treaty of European Union and the Treaty on the Functioning of the European Union [2016] C 202/01
[4] Information society services is defined as '… any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service …'. See, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 [17]
[5] Europa.eu, 'Regulations, Directives and other Acts' (*European Union*, 24 May 2018) <https://europa.eu/european-union/eu-law/legal-acts_en> accessed 9 July 2018
[6] For example, Article 25 of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, criminalises online child pornography.
[7] Commission n.1

directive) was adopted into EU law to help establish the boundaries of online service providers:

> 'Both existing and emerging disparities in Member States' legislations and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities …'.[8]

The directive governs several situations including, the creation of contracts online, the selling of goods *via* the use of the Internet and the liability of organisations which catches the activities of social media companies, in tackling terrorist-related material, child sexual abuse online and illegal hate speech. The directive puts an obligation on Member of States to ensure they put measures in place to achieve the purpose of the directive, whilst also allowing for freedom of speech to still be maintained across States. Consequently, only minimal implementation of the directive is needed to 'give effect to the proper functioning of the internal market'.[9]

The creation of the directive and its adoption into EU law has created several defences for online businesses. For instance, significant protection is given to social media companies under Article 14[10] of the directive.[11] Under Article

[8] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 [40]
[9] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 [10]
[10] A further two defences are contained in the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000. Article 12(1) protects internet service providers from liability for illegal content sent *via* their telecommunications network. Whereas Article 13(1) protects the storing of data by information society service providers.
[11] Lorna Woods, 'When is Facebook liable for illegal content under the E-commerce Directive? CG v. Facebook in the Northern Ireland courts' (*The International Forum for Responsible Media Blog*, 28 January 2017) <https://inforrm.org/2017/01/28/when-is-facebook-liable-for-illegal-content-under-the-e-commerce-directive-cg-v-facebook-in-the-northern-ireland-courts-lorna-woods/> accessed 10 July 2018

14(1) social media sites are considered under EU law as 'hosts' rather than 'publishers':

> 'Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service …'.

The purpose of the directive was to create consistency across EU Member of States in the regulation of information service providers, whilst also ensuring the development of the Internet, trade and the economy.[12] Put simply, information society services such as that of Twitter and Facebook cannot be held liable for conduct carried out on their sites as they are not considered the publishers of the information, they merely play host to the content. However, Article 14(2) imposes some limitations on this concept:

> 'a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.'[13]

From the evidence given it must be found that the provider had actual knowledge of the illegal content on its site. If sufficient knowledge is given, service providers must act 'expeditiously' to remove such content from its site, to rely on the defence of 'hosting'. If it can be established that the service provider in question had actual knowledge of the illegal content on its site and it did not act 'expeditiously' to remove such content, it can give rise

[12] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services
[13] Article 13(1) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000

to legal repercussions, as shown in *L'Oréal SA and Others v eBay International AG and Others*.[14]

In July 2011 a case was brought before the Court of Justice of the European Union following L'Oréal products being sold on the Internet selling site eBay without the companies consent. L'Oréal, a cosmetic based business had strict trademark regulations whereby its products could only be sold by companies who had gained the appropriate consent of the business. In the matter at hand a number of its products were being sold on eBay illegally, including sample bottles which were never intended for resale. The case originated in the High Court of the UK where a preliminary reference was made to the Court of Justice of the European Union.[15] Several issues were raised before the Court including the liability of eBay in the illegal activity, which was taking place on its website. In essence, the Court was asked two fundamental questions in relation to Article 14(1). First, did eBay fall within the definition of an 'internet service provider'; second, could it be considered that eBay had been made aware of the illegal content on its site?[16]

For the court, eBay could be considered as an online service provider and consequently could rely on the defence of being a 'host' rather than a 'publisher' as governed under Article 14(1) of the directive. However, the

[14] C-324/09 *L'Oréal SA and Others v eBay International AG and Others* [2011] ECLI 474
[15] A preliminary reference is '… the mechanism by which national courts and tribunals may (or in some cases must) seek definitive "rulings" from the CJEU [Court of Justice of the European Union] on the interpretation of EU legislation.' See, Steve Wilson, Helen Rutherford, Tony Storey & Natalie Wortley, *English Legal System* (2nd edn, Oxford University Press 2016) 202
[16] C-324/09 *L'Oréal SA and Others* n.14, [106]

Court of Justice of the European Union concluded that on numerous occasions eBay had been given constructive knowledge of the illegal activity being carried out on its site:

> 'Where, by contrast, the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31.'[17]

On several occasions eBay had actively advertised L'Oréal products through Google 'Ad Words'[18] making them fully aware of the illegal content on their marketplace. In addition, L'Oréal had written to eBay to express its growing concerns surrounding trademark products being sold on its site. As a result, the Court of Justice of the European Union concluded that the defence contained in Article 14(1) could not be relied upon.

The Court of Justice of the European Union has consequently set the limits for the defence of Article 14(1) though the judgment did not clarify a time limit for information service providers to remove illegal content. As previously stated under Article 14(1) when a company receives knowledge of an unlawful activity being carried out on its network, they must act 'expeditiously' to remove it. The directive does not define the term 'expeditiously', yet it has come to be accepted that it means within 24 hours, especially for social

[17] *Ibid.,* [116]
[18] Google AdWords is as system developed by the search engine Google where businesses can pay to display advisements online.

media companies.[19] Failure to comply with the removal of illegal content can result in an information society provider being in breach of the directive.

Despite the obligations put on providers to remove illegal content from its network upon constructive knowledge of its appearance, Internet services are not under a positive obligation to actively search for illegal activity, as affirmed in *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*:[20]

> 'In that regard, the Court has already ruled that the prohibition applies in particular to national measures which would require an intermediary provider, such as an ISP, to actively monitor all the data of each of its customers in order to prevent any future infringement … such a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48 [Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights], which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly …'.[21]

Scarlet concerned copyright-protected material, which was being illegally downloaded *via* the Internet service provider, Scarlet. SABAM, a management company representing authors, editors of music and composers brought an action against Scarlet for copyright infringements for allowing their customers to download material illegally without paying royalties. The the cour d'appel de Bruxelles (Belgium) concluded that Scarlet had breached copyright provisions; an injunction was granted against Scarlet to invest in technology, which would actively seek out customers who were

[19] Justice and Consumers, 'European Commission and IT Companies announce Code of Conduct on illegal online hate speech' (*European Commission*, 31 May 2016) <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=31811> accessed 10 July 2018
[20] C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECLI 771
[21] *Ibid.,* [36]

partaking in illegal behaviour online. The injunction was later overruled by the Court of Justice of the European Union who affirmed that Internet service providers were not under a legal obligation to actively seek out unlawful behaviour, or as potently put by Rizzuto:

> 'The Court of Justice ruled that national rules must, in particular, respect art.15(1) of Directive 2000/31, which prohibits national authorities from adopting measures which would require an internet service provider to carry out general monitoring of the information that it transmits on its network.'[22]

However, the advancement of technology has '… changed the way in which creative content is produced, distributed and accessed'.[23] Consequently, the European Parliament has recently voted in favour of implementing the Directive of The European Parliament and of The Council on Copyright in the Digital Single Market COM/2016/0593 (EU Copyright Directive). The EU Copyright Directive seeks to create copyright regulations suited to a digital age. In particular Article 13(1) states:

> 'Information society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users shall, in cooperation with rightholders, take measures to ensure the functioning of agreements concluded with rightholders for the use of their works or other subject-matter or to prevent the availability on their services of works or other subject-matter identified by rightholders through the cooperation with the service providers.'

In essence, information society service providers such as social media companies can now be held liable for copyright-protected material which is uploaded onto their sites.[24] Though the EU copyright directive does not place

[22] Francesco Rizzuto, 'Case Comment: Injunctions against intermediate online service providers' (2012) 18(3) Computer and Telecommunications Law Review 69, 71 (note)
[23] Commission, 'Questions and Answers – European Parliament's vote in favour of modernised rules fit for digital age' (*European Commission Press Release*, 30 April 2019) <http://europa.eu/rapid/press-release_MEMO-19-1849_en.htm> accessed 30 April 2019
[24] The EU Copyright Directive does give a list of companies who are not affected by the change in law, including, though not limited to, not-for-profit online encyclopaedias, open

an obligation on information society service providers to actively search for copyright-protected material, critics of this legal provision suggest that companies will have no choice but to actively search for material which breaches copyright regulations.[25]

The EU is consequently moving in the direction of better regulation of the Internet however these changes only currently apply to copyright-protected material. As a result, for all other behaviours companies must rely upon self-regulation, meaning inappropriate and unlawful material is flourishing online. Consequently, Members States of the European Union have witnessed a spread of terrorist material online in recent years, which has helped pave the way for non-binding measures to be imposed by the European Commission.[26]

In 2016 an online Code of Conduct was produced aimed at social media companies following terrorist attacks in Brussels.[27] The purpose of the Code of Conduct was to create a set of guidelines for social media companies to tackle illegal content online, in particular hate speech and terrorist propaganda.[28] The document places a number of obligations on social media companies including, specific guidelines for social media users, the removal of illegal hate speech within 24 hours and increased cooperation between

source software development platforms and cloud storage services'. See, BBC, Chris Fox, 'What is Article 13? The EU's copyright directive explained' *The BBC* (London, 14 February 2019) <https://www.bbc.co.uk/news/technology-47239600> accessed 27 March 2019

[25] *Ibid.,*

[26] Commission n.1. Note, this is not legally binding on social media companies.

[27] Justice and Consumers n.19

[28] Commission, 'European Commission and IT Companies announce Code of Conduct on illegal online hate speech' (*European Commission Press Release*, 31 May 2016) <http://europa.eu/rapid/press-release_IP-16-1937_en.htm> accessed 10 July 2018

social media companies.[29] The code of conduct only applies to companies who have agreed to its terms, including Facebook, Twitter and YouTube, known as the IT companies.

Despite the Code of Conduct not being legally binding on social media companies, 'significant progress has been made by the social platforms participating in the Code of Conduct'.[30] A study conducted a year after the Code of Conduct was adopted found that in 51.4% of cases, the IT companies removed illegal hate speech within 24 hours of being notified of its existence, an increase of 11.4% on the previous six months.[31] The mixed approach of binding and non-binding protocols used by the EU to help tackle online behaviour has had some positive impacts. The engagement of some social media sites in adhering to the Code of Conduct created by the European Commission is a significant step forward in combatting unlawful behaviour online. Nonetheless, problems have arisen following the emergence of the Facebook Cambridge Analytica scandal.[32]

As discussed in detail in chapter one, in March 2017 it became apparent that a major data breach had occurred within Facebook's network allowing Cambridge Analytica to harvest the personal data of 87 million Facebook

[29] *Ibid.,*
[30] Věra Jourová, 'Code of Conduct on countering illegal hate speech online: one year after' (*European Commission*, June 2017) <https://ec.europa.eu/newsroom/document.cfm?doc_id=40573> accessed 10 July 2018
[31] *Ibid.,*
[32] The Cambridge Analytical scandal as discussed in chapter one, concerns personal data, which was harvested from Facebook profiles without consent. The data collected was later used to target voters during political events across the globe. See, Patrick Greenfield, 'The Cambridge Analytica files: the story so far' *The Guardian* (London, 26 March 2018) <https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far> accessed 10 July 2018

users.[33] Therefore, posing the European Parliament to consider legislative provisions against social media companies:

> '"We are still working on the possible legal proposals … still stand on the position that for terrorism, extremism and images of child abuse we should have a more reliable framework that could introduce sanctions for lack of compliance … but the line between prohibiting hate speech and censorship is very thin."'[34]

The perspective of the European Parliament in endorsing legislation in tackling illegal conduct online is not mirrored by the European Commission. The European Commission instead promotes the use of non-legally binding protocols to curtail social media companies.[35] For example, strengthening the 'European Strategy for Better Internet for Children.'[36]

The European Strategy for Better Internet for Children was created by the Commission in 2012 following concerns about the exploitation of children online and issues surrounding cyberbullying. The paper puts forward several recommendations to social media companies to protect children online, including age-appropriate privacy settings.[37] This recommendation was accepted by Facebook who have separate privacy settings for minors including in-depth help pages for both children[38] and parents.[39] However, this

---

[33] See chapter one for an in-depth discussion on this.
[34] Věra Jourová EU commissioner for consumers and justice. See, Daniel Boffey, 'EU threatens to crack down on Facebook over hate speech' *The Independent* (London, 11 April 2011) <https://www.theguardian.com/technology/2018/apr/11/eu-heavy-sanctions-online-hate-speech-facebook-scandal> accessed 10 July 2018
[35]Jennifer Rankin, 'Tech firms could face new EU regulations over fake news' *The Guardian* (London, 24 April 2018) <https://www.theguardian.com/media/2018/apr/24/eu-to-warn-social-media-firms-over-fake-news-and-data-mining> accessed 24 July 2018
[36] Commission, 'European Strategy for a Better Internet for Children' COM (2012) 196 final
[37] *Ibid.,* 17
[38] Facebook, 'Youth Portal' (*Facebook*, 2018) <https://www.facebook.com/safety/youth> accessed 24 July 2018
[39] Facebook, 'Parents Portal' (*Facebook*, 2018) <https://www.facebook.com/safety/parents> accessed 24 July 2018

has not been reflected by other social media companies such as Twitter who continue to have the same default privacy settings for both adults and children.[40]

The absence of specific legal provisions placed on social media sites in combatting illegal content has resulted in a lack of consistency between social media companies. Ideas have been put forward by the European Commission to continue to reduce illegal behaviour online, but social media sites are not under a legal obligation to adhere to these recommendations. Put simply, companies such as Facebook and Twitter can choose to ignore the opinion of the European Commission. Consequently, 'a harmonised and coherent approach to removing illegal content does not exist across the EU.'[41]

Similarly, in England and Wales there is no true consensus on how to tackle the growing issue of online abuse. Several Parliamentary Committees have commenced in recent years examining abuse on social media sites, alongside the current criminal law framework. In 2014 the UK Communications Committee concluded that the criminal law governing social media was '… appropriate for the prosecution of offences committed using social media'.[42] Whereas in 2018 the Law Commission concluded that more needed to be done to successfully combat unlawful behaviour aided by

[40] Twitter, 'Twitter Rules Enforcement' (*Twitter*, 2018) <https://transparency.twitter.com/en/twitter-rules-enforcement.html#twitter-rules-enforcement-jan-jun-2018> accessed 18 February 2019
[41] Commission n.1, 5
[42] Communications Committee, *Social media and criminal offences* (HL 2014-15, 37) [5]

social media, including strengthening non-legislative provisions.[43] Consequently, like that of EU bodies, 'a harmonised and coherent approach to …' governing social media does not exist within England and Wales.

Australia

In Australia, the law is made up of several entities: The Constitution, Federal Law and State Law. Consequently, there are certain online conducts which are only criminalised in specific States of Australia rather than being a criminal offence across the country. This creates inconsistencies across States when it comes to tackling online behaviour. For example, in Victoria legislation is in place suited to the digital age,[44] whereas in Western Australia there are few legal provisions governing conduct carried out online.[45] As a result, States such as Western Australia must rely on the federal Criminal Code to tackle the growing issue of online abuse.

A body of law has been created by the Federal Government of Australia that relates to crime, the Criminal Code Act (1995) known as the Criminal Code. Under part 10.6 of the Criminal Code, offences related to telecommunications are criminalised including computer misuse,[46] the use of a telecommunications network to commit a serious crime,[47] and the prohibition of offensive material online.[48] These behaviours are similar to

[43] Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018)
[44] Parliament of Australia, *Cyber Safety - Joint Select Committee High-wire act: Cyber-safety and the young Interim report* (June 2011) [11.39]
[45] *Ibid.,* [11.48]
[46] Criminal Code Act (1995) section 476.2 (Australia)
[47] Criminal Code Act (1995) section 474.14 (Australia)
[48] Criminal Code Act (1995) section 474.17 (Australia)

legal provisions contained in the criminal law of England and Wales. Whereas in England and Wales, many legal provisions have been shaped and adapted to cover technology; the Federal Government of Australia has created legal provisions specifically aimed at governing online conduct.

Like that of England and Wales, it is a criminal offence in Australia to send, *via* a communications network, offensive material to another.[49] The law prohibiting offensive commentary sent online also criminalises the use of technology to menace and harass another:

> 'A person commits an offence if: (a) the person uses a carriage service; and (b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.'[50]

The Federal Government of Australia has specifically criminalised the conduct of online harassment. As outlined in chapter four cyber harassment is '… repeated attempts to impose unwanted communications and contact upon a victim in a manner that could be expected to cause distress or fear in any reasonable person'[51] pursued *via* the use of technology. Whilst in England and Wales harassment laws are based on a course of conduct that causes an individual alarm or distress,[52] in Australia the harassment of another is based on the concept of the reasonable person:

> 'The reasonable person test allows for community standards and common sense to be considered when determining whether certain conduct or content of a communication is menacing, harassing or of

[49] For example, the Communications Act 2003 section 127(1)
[50] Criminal Code Act (1995) section 474.17(1) (Australia)
[51] Home Office, 'Circular: a change to the Protection from Harassment Act 1997' (*Gov.uk*, 16 October 2012) <https://www.gov.uk/government/publications/a-change-to-the-protection-from-harassment-act-1997-introduction-of-two-new-specific-offences-of-stalking> accessed 27 July 2018
[52] Protection from Harassment Act (1997) section 1(1)

an offensive nature.'[53]

Consequently, the laws governing online harassment in Australia are wider than those found in the criminal law of England and Wales. As discussed in chapter four the concept that an individual must be alarmed or distressed by a course of conduct to invoke the Protection from Harassment Act 1997, means harassment is often misunderstood by the criminal justice system. As noted by Salter and Bryden the conduct of online harassment is 'disturbing, unpleasant and may transgress the norms of socially acceptable' behaviour, but it is difficult to prove that the conduct crosses a line to warrant criminal law intervention under the Protection from Harassment Act.[54]

In April 2019 the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill (the Bill) was put before the Australian Parliament, following a terrorist attack in Christchurch New Zealand, which killed 50 people.[55] The attack was livestreamed[56] on Facebook, later being removed by the company around an hour after the event occurred.[57] However, other Facebook users re-uploaded the video across social media sites.[58] In the first

[53] David Plater, '"Setting the boundaries of acceptable behaviour?" South Australia's latest legislative response to revenge pornography' (2016) 2 UniSA Student Law Review 77, 82
[54] Michael Salter & Chris Bryden, 'I can see you: harassment and stalking on the Internet' (2009) 18(2) Information & Communications Technology Law 99, 100
[55] Paul Karp, 'Australia passes social media law penalising platforms for violent content' *The Guardian* (London, 4 April 2019) <https://www.theguardian.com/media/2019/apr/04/australia-passes-social-media-law-penalising-platforms-for-violent-content?CMP=share_btn_tw> accessed 30 April 2019
[56] Livestreamed technology allows for online users to video share with other Internet users live. See, Facebook, 'Going Live on Facebook' (*Facebook*, 2019) <https://live.fb.com/about/> accessed 26 March 2019
[57] Jim Waterson, 'Facebook removed 1.5m videos of New Zealand terror attack in first 24 hours' *The Guardian* (London, 17 March 2019) <https://www.theguardian.com/world/2019/mar/17/facebook-removed-15m-videos-new-zealand-terror-attack> accessed 26 March 2019
[58] The BBC, 'Facebook: New Zealand attack video viewed 4,000 times' *The BBC* (London, 19 March 2019) <https://www.bbc.co.uk/news/business-47620519> accessed 26 March 2019

24 hours after the Christchurch attack, Facebook removed 1.5 million copies of the video from its site.[59] As a direct consequence of this event, the Australian Government proposed a Bill on 3 April 2019 for the purpose of creating a new criminal offence for social media service providers[60] that failed to remove abhorrent violent material, expeditiously.[61] The subsequent Bill received Royal Assent two days later.[62]

Under these new regulations, social media service providers need to remove videos that articulate terrorism, murder, attempted murder, torture, rape or kidnap[63] from their sites within a 'reasonable' and 'expeditious' time-limit.[64] Failure to comply with the Bill will either result in a $10.5 million fine (£5,652,622.50),[65] or in some cases, the imprisonment of company officials.[66] However, the Bill has been heavily criticised by the tech industry and politicians within Australia as a 'knee-jerk reaction to a tragic event.'[67]

---

[59] Waterson n.57

[60] Social media providers are defined as, 'an electronic service that satisfies the following conditions: the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users; the service allows end-users to link to, or interact with, some or all of the other end-users; the service allows end-users to post material on the service; such other conditions (if any) as are set out in the legislative rules'. Enhancing Online Safety Act 2015 section 9 (Australia)

[61] Parliament of Australia, 'Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019' (*Parliament of Australia*, 2019) <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1201> accessed 30 April 2019

[62] *Ibid.,*

[63] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019 section 474.32 (Australia)

[64] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019 section 474.34 (Australia)

[65] Or 10% of annual turnover.

[66] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019 section 474.34(10) and (11) (Australia)

[67] The Law Council of Australia president, Arthur Moses. See, Paul Karp, 'Australia passes social media law penalising platforms for violent content' *The Guardian* (London, 4 April 2019) <https://www.theguardian.com/media/2019/apr/04/australia-passes-social-media-law-penalising-platforms-for-violent-content?CMP=share_btn_tw> accessed 30 April 2019

Under the Bill several terms are included which are not specifically defined such as 'expeditiously' and 'reasonable time.' For Government officials who support the Bill it will be for the jury or the e-Safety Commissioner, discussed in detail in later parts of this section, to determine if abhorrent violent material has been removed from sites in a timely manner.[68] Subsequently, arguments have been put forward that the Bill is fundamentally 'flawed' putting at risk freedom of expression and legality in the criminal law.[69]

The creation of specific criminal offences suited to the digital age in Australia can be considered as a positive step forward in tackling unlawful behaviour online, though legislation needs to be passed with appropriate consideration, rather than a 'pass it now, change it later approach'.[70] However, it is important to note not all abusive online conduct is prohibited contrary to the Criminal Code in Australia. Instead, State Officials have had to enact their own legislation to criminalise behaviours such as revenge pornography.

In the State of Victoria, a person is prohibited from the sending of:

> '… an intimate image of another person (B) to a person other than B; and … the distribution of the image is contrary to community standards of acceptable conduct.'[71]

Whereas in England and Wales[72] the sender of the image must have distributed revenge porn to cause distress, in Victoria this element is not needed. Consequently, the laws prohibiting revenge pornography like that of

[68] *Ibid.,* per Attorney General, Christian Porter
[69] *Ibid.,* per The Chief Executive of Atlassian, Scott Farquhar.
[70] *Ibid.,* per Sunita Bose
[71] Summary Offences Act 1966 section 41DA(1) (Australia)
[72] For a discussion of revenge porn laws in England and Wales see chapter five.

the laws prohibiting online harassment in Australia, are significantly broader in Victoria as opposed to England and Wales. Similarly, in South Australia individuals can be held liable for the distribution of revenge pornography if they make available an 'invasive image of another person'[73] without the consent of the person in the picture. Here, the term 'invasive' is defined as a person:

> '(a) engaged in a private act; or (b) in a state of undress such that - (i) in the case of a female - the bare breasts are visible; or (ii) in any case - the bare genital or anal region is visible.' [74]

Despite the element of distress not being needed to prove a criminal offence in Victoria or South Australia, if the image in question can be considered to fall 'within the standards of morality, decency and propriety generally accepted by reasonable adults in the community', then it is unlikely that the conduct will be considered as revenge pornography.[75]

The fragmentation of the law across Australia means that not all citizens are protected under revenge porn laws.[76] Campaigns have started to emerge in Australia calling for the conduct of revenge pornography to be criminalised specifically under the Criminal Code,[77] especially for digital feminists such as

---

[73] Summary Offences Act 1953 section 26C(1) (Australia)
[74] Summary Offences Act 1953 section 26A(2) (Australia)
[75] Office of Legislative Drafting and Publishing, 'Guidelines for the Classification of Publications 2005: as amended' (*Gov.au*, 19 March 2008) <https://www.legislation.gov.au/Details/.../1ac3d219-38d6-4987-b21f-9e4b6ee27302> accessed 27 July 2018
[76] Arguments have been put forward that the Criminal Code of Australia prohibits revenge pornography, though this is disputed. See, Anastasia Powell, Asher Flynn & Nicola Henry, 'FactCheck Q&A: are there laws to protect against "revenge porn" in Australia?' *The Conversation* (London, 8 March 2017) <https://theconversation.com/factcheck-qanda-are-there-laws-to-protect-against-revenge-porn-in-australia-74154> accessed 27 July 2018
[77] For example, the office of the Commonwealth Director of Public Prosecutions in Australia has publicly supported a change in the criminal law in relation to revenge pornography. See, Lauren Wilson, 'Top prosecutor warns Australia's revenge porn laws are too weak to properly protect women' *news.com.au* (Sydney, 10 January 2016) <https://www.news.com.au/technology/online/security/top-prosecutor-warns-australias-

Powell and Henry.[78] The Federal Government of Australia has rejected this argument, instead suggesting that the offence should be prohibited under civil law as opposed to the criminal law.[79]

In February 2018 laws were passed through the Senate of Australia imposing fines of up to $105,000[80] Australian Dollars (£59,245) for those who distributed revenge pornography, which the reasonable person would consider inappropriate,[81] including photoshopped imagery. Currently, under the legal provisions prohibiting revenge pornography in England and Wales, photoshopped imagery is beyond the scope of section 33 of the Criminal Justice and Courts Act 2015. In essence, a fake image of a person engaging in a sexual activity, which is distributed to cause distress upon the person capsulated in the picture, is not currently prohibited under revenge porn laws in England and Wales. In Australia, a tough stance has been undertaken regarding the distribution of non-consensual imagery after Senates accepted that '… non-consensual sharing of intimate images is exploitative, it's humiliating and it's a very damaging form of abuse.'[82] Consequently, victims who have been subjected to revenge pornography can make a complaint to the Australian eSafety Commissioner.

---

revenge-porn-laws-are-too-weak-to-properly-protect-women/news-story/b597b7c0f1b0f76c7b7980ca545b512a> accessed 27 July 2018

[78] Anastasia Powell & Nicola Henry, *Sexual Violence in a Digital Age* (Springer 2017)

[79] The rationale for using the civil law to punish acts of revenge pornography is to ensure cases are dealt with quickly within the system, as complaints can be made directly to the eSafety Commissioner.

[80] Note, this is the fine for perpetrators of revenge pornography. Hosts of such content can be fined up to $525,000 (£296,226).

[81] AAP, 'Revenge porn bill passes Australian Senate' *news.com.au* (Sydney, 15 February 2018) <https://www.news.com.au/technology/online/revenge-porn-bill-passes-australian-senate/news-story/d911487ff7aa8b109f518d7ca0d72aa1> accessed 30 July 2018

[82] *Ibid.,*

The eSafety Commissioner is responsible for the promotion of Internet safety across Australia whilst also helping to tackle cyberbullying, illegal content online and revenge pornography.[83] Under the new non-consensual imagery based laws in Australia, victims of this form of behaviour are able to contact the Office of the eSafety Commissioner, who is then able to impose fines on both content hosts and the perpetrator to ensure images are removed from servers in a timely manner.[84] Despite a strong civil approach to tackling revenge pornography, the Nick Xenophon Team a political party based primarily in South Australia, called for the Act to also criminalise this type of conduct.[85] Whilst others opposed the recommendations put forward in the Act, fearing the construction of the law would threaten aspects of free speech, in particular satire communications: 'If I posted a picture or a drawing of President Donald Trump urinating in Central Park, I shouldn't face a $100,000 fine [*sic*].'[86]

Despite the lack of coherent legislation across Australia controlling conduct carried out online, States and the Federal Government have implemented several successful non-legislative approaches to help reduce cybercrime, including a National Cybercrime Working Group (NCWG). The purpose of the NCWG is to enable jurisdictions to work together in order to tackle cyber-related crime. Though the United Kingdom has a similar agency, the National

[83] Office of the eSafety Commissioner, 'Role of the Office' (*Australian Government*, 2018) <https://www.esafety.gov.au/about-the-office/role-of-the-office> accessed 30 July 2018
[84] AAP n.81
[85] *Ibid.,*
[86] Liberal Democrat Senator David Leyonhjelm. See, AAP n.81

Cyber Crime Unit governed by the National Crime Agency,[87] the NCWG has implemented an online policing strategy, whereby police officers are now present on social media sites. [88] In addition, the NCWG has adapted its approach to tackling unlawful behaviour online through its contribution towards educational campaigns.

In Australia educational initiatives to combat inappropriate conduct online are regarded as '… one of the most important elements of crime prevention'.[89] Programmes have been created by the Federal Government such as 'Thinkuknow',[90] targeting both school-aged children and the wider public.[91] Similarly, in the UK in September 2018 a compulsory national computer curriculum was made available in all state-based schools[92] to ensure:

> 'all young people are equipped to have healthy and respectful relationships in both the online and offline world, and leave school with the knowledge to prepare them for adult life.'[93]

The creation of a compulsory national computer curriculum is a positive step forward in the educational system, but its implementation comes 14 years after Facebook was made available to the wider public. Whereas the

[87] National Crime Agency, 'National Cyber Crime Unit' (*NCA*, 2018) <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit> accessed 27 July 2018
[88] Department of Home Affairs, 'Cybercrime' (*Australian Government*, 2017) <https://www.homeaffairs.gov.au/about/crime/cybercrime> accessed 27 July 2018
[89] Parliament of Australia n.44, [11.18]
[90] Thinkuknow, 'What we see, say, do online' (*Thinkuknow.org.au*, 2018) <https://www.thinkuknow.org.au/what-we-see-say-do-online> accessed 27 July 2018
[91] Parliament of Australia n.44 [11.18]
[92] Throughout the UK there are several ways in which schools are funded. Those not run by the state do not always have to follow changes implemented by the Government.
[93] HM Government, 'Government response to the Internet Safety Strategy Green Paper' (*Gov.uk*, May 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf > accessed 27 July 2018

'Thinkuknow' initiative was created in Australia in 2010, where in its first 9 months, 118 presentations were given to 4,450 individuals.[94]

Specific State programmes have also been created to tackle online abuse. For example, in the State of Victoria the Victorian Government has funded the first project aimed at addressing sexual abuse and violence against women online.[95] The purpose of the project, which is being led by Gender Equity Victoria, is to train users of the Internet to call out sexism, essentially creating a form of self-regulation online. Gender Equity Victoria aim to educate moderators based in media organisations to '… understand the gendered nature of violence', whilst also 'empowering' online users to tackle sexism.[96] In addition, recommendations were made by the Government of Australia to create a women's safety strategy.[97] Following the creation of the women's safety strategy an 'e-SafetyWomen' programme was also created by the e-Safety Commissioner, to 'empower Australian women to take control of their online experiences.'[98] The purpose of the programme is to allow women to gain the tools needed to help manage online abuse, whilst also creating reporting mechanisms for users. In essence, a victimological approach to online abuse has occurred throughout Australia, whereby the

[94] Parliament of Australia n.44, [11.18]
[95] Melissa Davey, 'Online sexism targeted in world-first "bystander" project' *The Guardian* (London, 31 May 2018) <https://www.theguardian.com/world/2018/jun/01/online-sexism-targeted-in-world-first-bystander-project> accessed 27 July 2018
[96] *Ibid.,*
[97] Department of the Prime Minister and Cabinet, '$100 million to help keep women safe' (*Australian Government*, 24 September 2015) <https://www.pmc.gov.au/news-centre/office-women/100-million-help-keep-women-safe> accessed 30 July 2018
[98] Office of the eSafety Commissioner, 'eSafetyWomen' (*Australian Government*, 2018) <https://www.esafety.gov.au/women/about-us> accessed 30 July 2018

victims have been placed at the centre of the criminal justice system.

The creation of an e-Safety Commissioner in Australia has been considered by the Australian Government as successful. Between its creation in 2015 and research conducted in 2017, the e-Safety Commissioner resolved 450 serious complaints of cyberbullying.[99] Furthermore, 19,000 cases were referred to other appropriate authorities, such as the police. The success of the e-Safety Commissioner was also reflected in the eSafetyWomen project, whereby in 2017, 2,000 frontline professionals across Australia were trained to help women who were being subjected to inappropriate behaviours online.[100] Individual States and the Federal Government of Australia are therefore attempting to tackle online abuse through a variety of different means.

Though there is some legislation in place which can be used to criminalise certain online conducts the law itself in Australia is fragmented. However, the non-legislative approaches to combatting online hate in Australia seems to be creating a precedent for other countries to follow. Whereas the European Union and Australia have been more inclined to use non-legislative provisions to control inappropriate behaviours online, the German Government has created legislation imposing specific obligations on social

[99] Senator the Hon Mitch Fifield, 'Esafety Commissioner to enhance online safety for all Australians' (*Senator the Hon Mitch Fifield*, 20 June 2017) <http://mitchfifield.com/Media/MediaReleases/tabid/70/articleType/ArticleView/articleId/1380/eSafety-Commissioner-to-enhance-online-safety-for-all-Australians.aspx> accessed 16 August 2018

[100] *Ibid.,*

media companies.

Germany

In 2017 the Federal Government of Germany passed the Act to Improve Enforcement of the Law in Social Networks, which became legally binding on 1 October of the same year.[101] The purpose of the Act was to impose punishments on social networking companies who were slow in their removal of illegal content online whilst also attempting to curtail 'fake' online news.[102]

Following a New Year's Eve celebration in Germany reports emerged online suggesting that Syrian refugees had been involved in disorderly conduct. The articles stated that 1,000 refugees had attacked police with fireworks, alongside setting a church alight.[103] In fact, no officers had been attacked and only a small fire had broken out damaging some nearby nets after a firework went off course. These reports were actively shared across social networking sites, attracting racist commentary despite the reports being untrue.[104]

[101] The Act was implemented in October 2017 however social media sites had three months from the implementation of the Act to comply with its conditions, before it became legally enforceable on 1 January 2018.
[102] Fake news can be defined '… as information distributed via a medium - often for the benefit of specific social actors - that then proves unverifiable or materially incorrect.' See, Simeon Yates, '"Fake news" – why people believe it and what can be done to counter it' *The Conversation* (London, 13 December 2016) <https://theconversation.com/fake-news-why-people-believe-it-and-what-can-be-done-to-counter-it-70013> accessed 31 July 2018.
[103] Will Worley, 'German police "shook heads in disbelief" at Breitbart News reporting of New Year's Eve events in Dortmund' *The Guardian (*London, 7 January 2017) <https://www.independent.co.uk/news/world/europe/breitbart-news-dortmund-police-new-years-eve-fake-news-germany-angela-merkel-syrians-refugee-crisis-a7514786.html> accessed 31 July 2018
[104] Consequently, these reports were then being used to justify hatred, racism and campaigns requesting the removal of refugees from Germany by online users.

The spread of fake news surrounding the events of 31 December 2016 led the Federal Government of Germany to come to a decision to legislate against fake news and online hate,[105] after concluding that:

> 'Online discussions are often aggressive, abusive and hateful … Hate crime may seriously threaten the peace in a liberal, open and democratic society if it's not suppressed and prosecuted effectively.'[106]

Consequently, the German Government implemented the Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) 2017. The Network Enforcement Act applies:

> '… to telemedia service providers which, for profit-making purposes, operate Internet platforms which are designed to enable users to share any content with other users or to make such content available to the public ...'.[107]

The purpose of the Act is to place obligations on social media sites to remove or block unlawful content in the State of Germany. Following the implementation of the Network Enforcement Act, Facebook had to employ 10,000 new moderators to help tackle online hate.[108]

For content to be considered as unlawful under the Network Enforcement Act it must breach the German Penal Code.[109] Like that of Australia, Germany

---

[105] Lizzie Dearden, 'Germany to fine social networks up to €50m for not taking down illegal "fake news" posts' *The Independent* (London, 5 April 2017) <https://www.independent.co.uk/news/world/europe/germany-fake-news-social-networks-fine-facebook-50-million-euros-illegal-content-hate-speech-angela-a7668731.html> accessed 31 July 2018

[106] Federal Ministry of Justice and Consumer Protection, 'Questions and answers: Act to Improve Enforcement of the Law in Social Networks' (*German Government*, 2017) <https://www.bmjv.de/SharedDocs/FAQ/EN/NetzDG/NetzDG.html> accessed 31 July 2018

[107] Act to Improve Enforcement of the Law in Social Networks (2017)

[108] The Local, 'This is what Facebook moderators in Germany have to deal with' *The Local* (Stockholm, 16 December 2016) <https://www.thelocal.de/20161216/this-is-what-facebook-moderators-in-berlin-have-to-deal-with> accessed 31 July 2018

[109] Act to Improve Enforcement of the Law in Social Networks (2017) section 1(3). See also, Federal Ministry of Justice and Consumer Protection n.106

has codified the criminal law into one document. Under the German Penal Code, a total of twenty-two behaviours are criminalised which are considered to be applicable in an online context. For instance, incitement of hatred,[110] revenge pornography[111] and defamation.[112] Here, under the Network Enforcement Act, social media companies must remove or block[113] content which can be considered to breach the Penal Code.[114]

The specified time limit for social media companies to remove illegal content from its sites in Germany is dependent upon the classification of the unlawful content. The Act places different time constraints on the removal of 'manifestly unlawful content' and content which is simply 'unlawful'. 'Manifestly unlawful content' must be removed or blocked from sites within 24 hours of being 'flagged'.[115] Whereas content which is considered as 'unlawful' contrary to the German Penal Code, must be removed within seven days.[116] Yet the Act does not clarify the difference between 'manifestly unlawful content' and 'unlawful content'.

As explored in detail in chapter two the principle of legality in the criminal law is the concept that legal provisions need to be definable, clear and accessible in order for citizens to adhere to the law. Like that of the UK,

[110] German Criminal Code (Strafgesetzbuch) section 130
[111] German Criminal Code (Strafgesetzbuch) section 201a
[112] German Criminal Code (Strafgesetzbuch) section 166, 185, 186 & 187
[113] Content which is simply blocked results in the communication not being publicly viewable within the Federal State of Germany. Whereas communications which are deleted, are no longer viewable across the globe. See, Federal Ministry of Justice and Consumer Protection, n.106
[114] Act to Improve Enforcement of the Law in Social Networks (2017) section 3(2) (Germany)
[115] 'Flagged' is a term used to describe when a communication online has been reported to the network host.
[116] Act to Improve Enforcement of the Law in Social Networks (2017) section 3(3) (Germany)

Germany is a signatory to the European Convention on Human Rights and Fundamental Freedoms (the Convention). The ambiguity of the terms 'manifestly unlawful' and 'unlawful' breaches the concept of legality within the criminal law. The Act contains no definition of the two terms yet social media sites must clearly differentiate between the two types of conducts to adhere to the law. Failure to comply with these time limits can result in a company being issued with a heavy fine,[117] whilst putting a person's right to freedom of speech at risk:

> 'The distinction between "manifestly unlawful" and "unlawful" is not clear, and difficult for a private enterprise to accurately predict: the Act provides no guidance to Social Networks on how they should differentiate "manifestly unlawful content" from "unlawful content", and contains no duty on the part of Social Networks to consider user's rights to freedom of expression when making these determinations (even though law enforcement authorities are required to consider this when acting to restrict freedom of expression pursuant to the GCC [German Criminal Code]).'

In Germany, freedom of speech is protected under both Article 10 of the Convention and under Article 19 of the Universal Declaration of Human Rights, enforced by Article 19 of the International Covenant on Civil and Political Rights. Like that of Article 10 of the Convention, as explained in detail in the previous chapter, Article 19 is a qualified right and can be restricted when certain criterions are met: the restriction is governed by law, the restriction pursues one of the legitimate aims found under the Article, and the restriction is necessary in a democratic society. Yet the Network Enforcement Act contains no safeguards for freedom of speech, in fact social media companies are under no legal obligation to take into account a

[117] Act to Improve Enforcement of the Law in Social Networks (2017) section 4 (Germany)

person's right to freedom of expression when removing content which they consider to breach the German Penal Code.[118]

For the campaign group 'ARTICLE 19' the new social media laws in Germany, violates a citizen's right to freedom of expression:

> 'ARTICLE 19 finds the Act, taken overall, to be dangerous to the protection of freedom of expression in Germany, and we are particularly concerned that countered with much weaker institutional and legal safeguards for the protection of human rights are looking at this Act as a model for increasing intermediary liability.'[119]

The Network Enforcement Act for ARTICLE 19 requires social media sites to act too quickly in the removal of content from its servers. Consequently, there is no guidance in place to protect freedom of speech. Therefore, social media sites are more likely to be over-cautious creating an '… environment wherein lawful content is routinely blocked or removed as a precaution.'[120] This perspective has been supported further by David Kaye, the UN's Special Rapporteur on freedom of expression:

> 'With these 24 hour [to] seven day deadlines - if you are a company you are going to want [to] avoid fines and bad public branding of your platform. If there is a complaint about a post you are just going to take it down. What is in it for you to leave it up? I think the result is likely to be greater censorship.'[121]

Following the implementation of the Network Enforcement Act several individuals in Germany had their social media accounts blocked by social

---

[118] Whereas the Courts of Germany must take into account a person's right to free speech.
[119] ARTICLE 19, 'Germany: The Act to Improve Enforcement of the Law in Social Networks' (*article19.org*, August 2017) 24 <https://www.article19.org/wp-content/uploads/2017/09/170901-Legal-Analysis-German-NetzDG-Act.pdf> accessed 13 July 2018
[120] *Ibid.,* 1
[121] David Kaye, the UN's Special Rapporteur on Freedom of Expression. See, Patrick Evans, 'Will Germany's new law kill free speech online?' *The BBC* (London,18 September 2017) <https://www.bbc.co.uk/news/blogs-trending-41042266> accessed 31 July 2018

media companies.[122] For example, Beatrix von Storch the leader of the far-right Alternative German Party, had her account blocked by Twitter for 12 hours after posting the following tweet: 'Are they seeking to appease the barbaric, Muslim, rapist hordes of men?'[123] Consequently, the changes in the law in Germany has resulted in companies being overly cautious for fear of being fined.[124]

Not only has the Act created an obligation on social media companies to remove unlawful content within a given time period, but social media companies must now also produce six-monthly reports detailing their approaches to the removal of illegal content:

> 'Providers of social networks which receive more than 100 complaints per calendar year about unlawful content shall be obliged to produce half-yearly German-language reports on the handling of complaints about unlawful content on their platforms … and shall be obliged to publish these reports in the Federal Gazette and on their own website no later than one month after the half-year concerned has ended. The reports published on their own website shall be easily recognisable, directly accessible and permanently available.'[125]

The Act goes further to list the minimum information which needs to be included within the report, for instance: how users can submit complaints of unlawful behaviour,[126] how many complaints were made in a given period[127]

---

[122] Philip Oltermann, 'Tough new German law puts tech firms and free speech in spotlight' *The Guardian* (London, 5 January 2018) <https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight> accessed 6 August 2018

[123] Joseph Nasr, 'Beatrix von Storch: German police accuse AfD politician of hate incitement over anti-Muslim tweet' *The Independent* (London, 2 January 2018) <https://www.independent.co.uk/news/world/europe/beatrix-von-storch-germany-afd-anti-muslim-twitter-north-rhine-westphalia-new-years-eve-a8138086.html> accessed 31 July 2018

[124] Oltermann n.122

[125] Act to Improve Enforcement of the Law in Social Networks (2017) section 2(1) (Germany)

[126] Act to Improve Enforcement of the Law in Social Networks (2017) section 2(2)2 (Germany)

[127] Act to Improve Enforcement of the Law in Social Networks (2017) section 2(2)3 (Germany)

and the time taken to remove unlawful content.[128] This is a similar approach undertaken by the European Commission through their 'Code of Conduct'. As stated previously the European Commission has imposed a non-legally binding code of conduct on social media sites, to remove illegal content within 24 hours. Similarly, reports are produced to examine social media companies compliance with this non-legislative approach to tackling hate speech online. However, Germany has now placed obligations on the likes of Facebook and Twitter to legally comply with the creation of reports detailing online abuse on its sites, or risk being issued with a fine of up to 500,000 euros (£453,557).[129] A deterrence effect has therefore been created by German authorities, although the deterrence aspect is aimed at social media companies as opposed to the user.

The final decision on the fine posed on a company will be made by the Federal Ministry of Justice and Consumer Protection, with the backing of the Federal Ministry of the Interior and the Federal Ministry for Economic Affairs and Energy.[130] Though the authority must also obtain a ruling by the German Administrative Court that the content in question is unlawful, adding some protection for freedom of expression.[131] The extent of the fine will be dependent upon the condition which has been breached, as set out in

[128] Act to Improve Enforcement of the Law in Social Networks (2017) section 2(2)8 (Germany)
[129] Act to Improve Enforcement of the Law in Social Networks (2017) section 4(2) (Germany)
[130] Act to Improve Enforcement of the Law in Social Networks (2017) section 4(4) (Germany)
[131] Act to Improve Enforcement of the Law in Social Networks (2017) section 4(5) (Germany)

section 4 of the Act. For example, a failure to name a representative based in Germany[132] can result in a fine of up to 50 million euros (£45,341,155).[133]

The implementation of the Network Enforcement Act in Germany has created opposing opinions. Pro-freedom of speech activists argue that the Act breaches the fundamental principles of freedom of expression, as companies will be more inclined to remove online content which may be borderline unlawful.[134] For ARTICLE 19 not only does the Network Enforcement Act limit a person's freedom of speech, the Act does not comply with the fundamental principle of legality in the criminal law. For ARTICLE 19 the Network Enforcement Act contains a variety of ambiguous wording, including what constitutes a social network.[135]

Social networks are defined under the Act as:

> '… telemedia service providers which, for profit-making purposes, operate Internet platforms which are designed to enable users to share any content with other users or to make such content available to the public (social networks).'[136]

For ARTICLE 19 the use of the terms 'sharing' or making content 'available' brings platforms, which would be traditionally not defined as 'social networks', into the reach of the Act. For instance, gaming platforms, instant messaging websites or websites whereby users can leave product reviews,

[132] Under section 5 of the Network Enforcement Act, all social media companies have to name a dedicated person who will answer any issues the German Government incur.
[133] Act to Improve Enforcement of the Law in Social Networks (2017) section 4(2)
[134] Johanna Spiegel, 'Germany's Network Enforcement Act and its impact on social networks' (*TaylorWessing*, 2018) <https://www.taylorwessing.com/download/article-germany-nfa-impact-social.html> accessed 27 June 2019
[135] ARTICLE 19 n.119, 12-13
[136] Act to Improve Enforcement of the Law in Social Networks (2017) section 1 (Germany)

could be considered as social media under the Network Enforcement Act.[137] The German Government has attempted to clarify the position of some online services:

> 'Platforms with journalistic/editorial content are also excluded. This also applies to websites that use the infrastructure of another social network to make their own journalistic/editorial content available, e.g. in the form of a Facebook page or profile.'[138]

Limitations have therefore been placed on the overall reach of the Act, whereby blogs and journalistic content are exempt from the conditions set out within the Network Enforcement Act.[139]

The Network Enforcement Act has created mixed debates since its implementation into the legal system of Germany. The law tackles the hosts of unlawful content, rather than the publisher, putting the onus on companies to remove illegal content from its sites rather than pursuing the individual who posted such commentary. This approach differs from England and Wales. Currently, the criminal law in England and Wales governing social media conduct focusses on targeting the perpetrator of unlawful behaviour, as opposed to the social media company hosting the comment. Likewise, in India, the Indian Government has implemented legislation aimed at the online user.

[137] ARTICLE 19 n.119, 12-13
[138] Federal Ministry of Justice and Consumer Protection n.106
[139] In addition, social networking sites who have less than two million users in the State of Germany are also exempt from prosecution under the Act. Act to Improve Enforcement of the Law in Social Networks (2017) section 1(2) (Germany)

India

Like that of Germany, India has taken a strong stance towards controlling unlawful behaviour online. In 2000 Indian authorities enacted the Information Technology Act, with the Act being updated in 2008.[140] Unlike Germany, India has attempted to combat unlawful conduct online, rather than targeting website hosts. The purpose of the Information Technology Act was to create one specific Act of Parliament criminalising cybercrime.[141] The Act also encompasses provisions from the Indian Criminal Code, in an attempt to make it more compatible with the advancements of changing technology.[142]

The Information Technology Act is based on the United Nations Model Law on Electronic Commerce 1996,[143] whilst also mirroring many provisions contained in the law of England and Wales. For example, under section 67 of the Act citizens are prohibited from the sending of:

> '… material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it …'.

Section 67 contains similar provisions to the Obscene Publications Act 1959 and 1964 in England and Wales, whereby communications which can be considered to deprave or corrupt a person are criminalised. However, this

[140] Ministry of Electronics & Information Technology, 'Information Technology Act 2000' (*Government of India*, 2018) <http://meity.gov.in/content/information-technology-act-2000> accessed 8 August 2018
[141] Information Technology Act 2000 section 1 (India)
[142] Krishna Deo Gaur, *Textbook on the Indian Penal Code* (Universal Law Publishing 2009) 57-58
[143] Abhilash CM, 'E-Commerce Law in Developing Countries: An Indian Perspective' (2002) 11(3) Information & Communications Technology Law 269

provision contained in the Information Technology Act has come under heavy criticism following its use to censor freedom of speech within India.

Research undertaken by 'Point of View', a not-for-profit based organisation in India, has uncovered a growing trend in the use of section 67 to curtail political speech over the last few years:

> '2015 was a bumper year for Section 67. A state in India secured its first-ever IT Act conviction - under this section. A case was filed against India's most famous porn actress - under this section. A comedy crew was booked [prosecuted] for roasting famous Bollywood stars. And a few individuals were charged with making fun of politicians - all under this section.'[144]

In the same year an Indian citizen Ajay Hatewar was charged for both the sending of a defamatory communication contrary to section 67A of the Act, alongside a second charge under section 67, after posting a tweet aimed at the Chief Minister of Maharashtra, Devendra Fadnavis.[145] The tweet in question simply contained a photo of Devendra Fadnavis on a yacht with his family, yet it was considered by the authorities as obscene. At no point could it be considered that the photo would deprave or corrupt those who viewed it.[146] Section 67 of the Information Technology Act has therefore been used to limit political discourse throughout India:

> 'From 2015 to 2017, Section 67 was used for censoring tweets, posts and content which spoke out against politicians. More often than not, this content was not obscene.'[147]

---

[144] Bishakha Datta *et al,* 'Guavas and Genital: A research study in Section 67 of the Information Technology Act' (*Point of View*, 2017) 4 <https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Smita_Vanniyar.pdf> accessed 8 August 2018
[145] Venkat Narayan, 'Man booked under IT Act for "defaming" CM Devendra Fadnavis' *The Times of India* (Mumbai, 10 July 2015) <https://timesofindia.indiatimes.com/india/Man-booked-under-IT-Act-for-defaming-CM-Devendra-Fadnavis-in-tweet/articleshow/48011122.cms> accessed 8 August 2018
[146] Datta *et al* n.144, 12
[147] *Ibid.,* 11

Like that of section 67 of the Information Technology Act, section 66A of the Act was created based on similar legislation contained in the criminal law of England and Wales:

> 'Any person who sends, by means of a computer resource or a communication device (a) any information that is grossly offensive or has menacing character; or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device [will be prosecuted]'.

The format of section 66A stems from section 127 of the Communications Act 2003 and the Malicious Communications Act 1988, however it has been expanded to cover specific situations. This section was substituted into the Information Technology Act in 2008 following arguments that the law did not adequately protect individuals from online abuse.[148] The purpose of section 66A was to criminalise the conduct of sending grossly offensive, menacing or false messages online. Like that of section 67 of the Act, it was later used to restrict freedom of expression in India.

Following the death of a controversial political figure, Bal Thackeray, Shaheen Dhada took to Facebook to express her opinion on the subsequent shutdown of a major city in India:

> 'Every day thousand[s] of people die. But still the world moves on ... Just due to one politician dead. A natural death. Everyone goes crazy ... Respect is earned not given out, definitely not forced. Today Mumbai shuts down due to fear not due to respect'.[149]

[148] Seema Chishti, 'Prescription post Section 66A: "Change law to punish hate speech online"' *The Indian Express* (New Delhi, 6 October 2017) <https://indianexpress.com/article/india/hate-speech-online-punishment-supreme-court-section-66a-information-technology-act-narendra-modi-4876648/> accessed 8 August 2018

[149] Rajini Vaidyanathan, 'India Facebook arrests: Shaheen and Renu speak out' *The BBC* (London, 26 November 2012) <https://www.bbc.co.uk/news/world-asia-india-20490823> accessed 8 August 2018

Soon after she posted the message on Facebook Dhada received phone calls from friends telling her to remove the message. Later the same day, she was arrested for her own safety after supporters of Thackeray took offence to the Facebook post. The following day after being held in a police cell overnight, Dhada was rearrested for violating section 295a of the Indian Penal Code. However, she was subsequently charged under section 66A of the Information Technology Act. In addition, a friend of Dhada, Renu Srinivasan, was also charged for the same offence under the Information Technology Act for liking, sharing and commenting on the original post.[150]

In India a person's right to free speech is protected under Article 19(1) of the Constitution of India 1949: 'All citizens shall have the right … to freedom of speech and expression …'. Like that of Article 10 of the Convention, freedom of expression can be limited by the state of India:

> '… in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence.'[151]

Only in the circumstances above can Indian authorities limit a person's right to freedom of speech. Failure to comply with these conditions and the Indian Constitution can result in the Supreme Court of India striking down a provision contained within an Act, as demonstrated in *Shreya Singhal v Union of India*.[152]

[150] *Ibid.,*
[151] The Constitution of India 1949 Article 19(2)
[152] *Shreya Singhal v Union of India* (2013) 12 S.C.C. 73

The *Shreya Singhal* case stemmed from nine writ petitions filed under Article 32 of the Indian Constitution: 'Right to Constitutional Remedies'.[153] The Supreme Court in this matter was asked to consider a number of issues, including the compatibility of section 66A of the Information Technology Act with Article 19 of the Constitution, a person's right to free speech. In addition, the court also examined if section 66A was clear and predictable therefore complying with the principles of legality in the criminal law. For Judge Natiman:

> '… a penal law is void for vagueness if it fails to define the criminal offence with sufficient definiteness. Ordinary people should be able to understand what conduct is prohibited and what is permitted. Also, those who administer the law must know what offence has been committed so that arbitrary and discriminatory enforcement of the law does not take place.'[154]

Consequently, the court looked at the key terms of section 66A in detail, including the prohibition of grossly offensive and menacing material being sent *via* a communications network.

As previously stated, section 66A is built on the provisions contained in the Malicious Communications Act and section 127 of the Communications Act. Like that of the Malicious Communications Act and section 127 of the Communications Act, section 66A does not define the terms 'grossly offensive' or 'menacing'.[155] For the Supreme Court of India this raised concerns that the terms were ambiguous, and consequently did not comply with the principles of legality:

---

[153] In essence, under this Article the Supreme Court of India has the right to rule on the compliance of an Act with the Constitution of India.
[154] *Shreya* n.152, [56]
[155] For further discussion on this point see chapter six.

> ‘Quite apart from this, as has been pointed out above, every expression used is nebulous in meaning. What may be offensive to one may not be offensive to another. What may cause annoyance or inconvenience to one may not cause annoyance or inconvenience to another. Even the expression “persistently” is completely imprecise - suppose a message is sent twice, can it be said that it was sent “persistently”? Does a message have to be sent (say) at least eight times, before it can be said that such message is “persistently” sent? There is no demarcating line conveyed by any of these expressions - and that is what renders the Section unconstitutionally vague.’

Here, the Supreme Court examined in detail two cases from English Law: *Director of Public Prosecutions v Collins*[156] and *Chambers v Director of Public Prosecutions*.[157]

For the Supreme Court of India, the cases of *Collins* and *Chambers* provided evidence of the ambiguity of the terms ‘grossly offensive’ and ‘menacing’:

> ‘These two cases illustrate how judicially trained minds would find a person guilty or not guilty depending upon the Judge’s notion of what is “grossly offensive” or “menacing”. In Collins’ case, both the Leicestershire Justices and two Judges of the Queen’s Bench would have acquitted Collins whereas the House of Lords convicted him. Similarly, in the Chambers case, the Crown Court would have convicted Chambers whereas the Queen’s Bench acquitted him. If judicially trained minds can come to diametrically opposite conclusions on the same set of facts it is obvious that expressions such as “grossly offensive” or “menacing” are so vague that there is no manageable standard by which a person can be said to have committed an offence or not to have committed an offence.’[158]

The lack of a clear definition for the key terms, ‘menacing’ and ‘grossly offensive’, led the Supreme Court of India to conclude that section 66A of the Information Technology Act did not comply with the notion of legality in the criminal law. In addition, the Court supported the argument that section 66A provided no safeguards for freedom of speech and conflicted with Article 19

[156] *Director of Public Prosecutions v Collins* [2006] UKHL 40
[157] *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin), [2013] 1 WLR 183
[158] *Shreya Singhal* n.152, [82]

on the Indian Constitution. Consequently, this particular section of the Information Technology Act was considered as void by the Supreme Court and struck down.[159]

The judgment of the Supreme Court in *Shreya Singhal* has removed section 66A from the Information Technology Act meaning it can no longer be used in the criminal justice system of India. One of the overriding rationales for striking down section 66A concerned issues of legality, using the cases of *Collins* and *Chambers* to support their judgement. Yet in England and Wales authorities continually use the Malicious Communications Act and section 127(1) of the Communications Act to prosecute social media offences, despite no clear definition contained in English law in relation to 'grossly offensive' and 'menacing' communications. As argued in chapter six the lack of a clear understanding as to the meaning of these terms can create inconsistencies in the criminal justice system, as demonstrated clearly in *R v Alison Chabloz*.[160]

Whereas in England and Wales it can be suggested that there seems to be a failure to act on complaints of online abuse, in India, authorities are using the Information Technology Act to the extreme to curtail free speech, through the use of deterrence. Since the implementation of the Information Technology Act, the law has been heavily criticised for its use by authorities.[161]

---

[159] *Ibid.,* [119]
[160] *R v Alison Chabloz* Westminster Magistrates' Court 25 May 2018 (unreported)
[161] Richa Kaul Padte, 'Keeping women safe? Gender, online harassment and Indian law' (*Internet Democracy Project*, 29 June 2013) <https://internetdemocracy.in/reports/keeping-women-safe-gender-online-harassment-and-indian-law/> accessed 14 August 2018

Consequently, Indian authorities have a long way to go before it can be said that they are striking a balance between online abuse and freedom of expression.

Chapter Overview

There is no one singular approach to containing unlawful conduct carried out online. The European Union has attempted to create a coherent approach across all Members of States through directives, but illegal content is on the rise. The growing use of social media has raised criticism from the European Parliament who have called for social media companies to do more.[162] Recently, Mark Zuckerberg the founder of Facebook, has been before the European Parliament and the Commission where he was posed questions from Members of the European Parliament (MEPs), about what his company was doing to curtail unlawful behaviour and fake news online. During the conversations with MEPs, Zuckerberg was warned about the powers his company possesses:

> 'You have to ask yourself how you will be remembered - as one of the three big Internet giants together with Steve Jobs and Bill Gates who have enriched our worlds and our societies. Or on the other, in fact, a genius who created a digital monster that is destroying our democracies and our societies.'[163]

Despite the power social media companies have across the globe, the European Commission has maintained its stance in strengthening non-

[162] Alexis C Madrigal, 'A Belgian Legislator Berates and Scoffs at Mark Zuckerberg' *The Atlantic* (Boston, 22 May 2018) <https://www.theatlantic.com/technology/archive/2018/05/a-belgian-legislator-berates-and-scoffs-at-mark-zuckerberg/560960/> accessed 16 August 2018
[163] *Ibid.,*

legislative approaches to reducing unlawful behaviour online. This is a similar approach endorsed in Australia.

For those countries who have taken a legislative approach to tackle illegal online behaviour, two main criticisms have been raised: freedom of speech and legality. Free speech is an important aspect of any democratic state, as upheld by the European Court of Human Rights:

> 'Freedom of expression constitutes one of the essential foundations of such a society, one of the basic conditions for its progress and for the development of every man.'[164]

As explored in the previous chapter freedom of speech is a fundamental legal principle which needs to be maintained but, there is a boundary between freedom of expression and interfering with a person's privacy. The examples given above illustrate the difficulties lawmakers have in creating legislation which curtails unlawful behaviour online, whilst also maintaining free speech in a democratic society. However, the main problem with legal provisions which have been implemented in India and Germany concerns the principle of legality in the criminal law.

The principle of legality ensures that all criminal law provisions are clear, certain and accessible. In India the Supreme Court has struck down legislation used to curtail online behaviour after it was considered that the terms 'menacing' and 'grossly offensive' were ambiguous, yet in England and Wales similar laws remain in place. Whereas in Germany the Network Enforcement Act is a relatively new piece of legislation, and therefore it

[164] *Handyside v United Kingdom* (1976) 1 EHRR 737 [49]

remains to be seen if the Act will be upheld as being constitutionally viable. It will be for future cases which are brought before the German Judiciary to establish if the Network Enforcement Act complies to the principles of legality in the criminal law.

From the discussion above a mixed-method approach is needed to help combat the growing issues of unlawful conduct online. Non-legislative approaches allow digital education to be strengthened within society. Nonetheless, this needs to be done alongside further changes in the legal system. Germany has paved the way for specific social media laws, but it is far from perfect.

Chapter eight: Recommendations

- Create a harmonised approach between legislation and non-legislative provisions governing online abuse;
- Ensure social media companies are held to account for abusive content facilitated by their sites in the form of a fine;
- Create better educational schemes for children, parents and law enforcement relating to digital literacy skills;
- Create clear and precise legal rules regulating online conduct and abuse in the form of a coherent Act of Parliament, whilst also ensuring provisions are in place to protect freedom of expression;
- The creation of an e-Safety Commissioner in the UK overseeing the regulation of social media companies, a digital authority and

educational schemes aimed at law enforcement, school children and parents;

- Define grossly offensive and menacing material with the aid of case law examples and the Crown Prosecution Service guidelines on social media prosecutions; and
- Create a transparent reviewing system of all legal provisions implemented to govern social media abuse to ensure democracy is maintained and freedom of speech is not curtailed.

Chapter Nine

Recommendations

> 'Since its inception, the Internet has been an amazing force for good. It has had an extraordinary impact on people around the globe. It has created lines of communication; driven innovation, growth and new business models; and, it has connected and given a voice to the previously disenfranchised. For the first time ever, anyone, anywhere, with a smartphone and an internet connection can grow their own business and connect with people from around the world … but as the Internet has developed, risks have emerged online and behaviours that would not be tolerated in the real world are increasingly condoned online.'[1]

This thesis set out to examine how the current criminal law framework of England and Wales governs online abuse aided by social media, and the law's adequacy in protecting those subjected to abuse online. The previous chapters have exposed several issues with the current criminal law framework and its use in a social media setting. Using the issues highlighted throughout this thesis recommendations will be put forward in the following discussion as to how the criminal justice system, and society can better protect victims of online abuse.

In recent years reports have been conducted by the Government, parliamentary committees and not-for-profit organisations examining different aspects of online abuse. In April 2019 the UK Government released an 'ambitious' White Paper on Online Harms (the White Paper),[2] supporting the idea that a '… new regulatory framework' was needed to ensure the UK

[1] HM Government, 'Internet Safety Strategy – Green paper' (*Gov.uk*, October 2018) 2 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf > accessed 19 March 2019
[2] HM Government, *Online Harms White Paper* (CP 57, 2019) 1

becomes '… the safest place in the world to go online.'[3] The recommendations put forward by the Government mirror some of the recommendations suggested in this chapter, but there are also some key differences; a comparison between the two will occur throughout the discussion below.

The Criminal Justice System

The previous chapters have exposed continuing issues with how the criminal justice system currently tackles abusive behaviour online. Arguments have been put forward concerning the legality of the current criminal law framework and its application in a social media setting. As highlighted in chapters four and six the use of the Public Order Act 1986, the Serious Crime Act 2007, the Protection from Harassment Act 1997, the Malicious Communications Act 1988 and section 127 of the Communications Act 2003, in a social media context, does not always conform to the principle of legality in the criminal law.

Issues have also been highlighted at various points in this thesis concerning the current approach law enforcement and the Crown Prosecution Service (CPS) have taken in matters relating to online abuse. For instance, Caroline Criado-Perez as discussed in chapter four, has been highly critical of the criminal justice systems approach to the continued online abuse she was subjected to in 2013 by Peter Nunn:[4]

[3] *Ibid.,* [1]
[4] For an in-depth discussion of this case see chapter four.

> ‘This man [Peter Nunn] made me fear for my life as no-one ever has before. I felt he was a clear and present threat to me. He made me scared to go outside, to appear in public. He stopped me being able to sleep; being able to work. He seemed obsessed enough to carry out his threats. I am glad he has been found guilty [of sending grossly offensive messages contrary to section 127(1) of the Communications Act]. I am glad he cannot contact me again. I hope he has learnt from this. But I think the CPS got the charge wrong. I don’t feel they understood what happened to me.’[5]

The conduct of Peter Nunn, in sending abusive messages to Ms Criado-Perez, might be thought to be more serious than the crime for which he was convicted - sending indecent, obscene or menacing messages - for which he received a six week custodial sentence.[6] Rather, it might be thought that his actions amounted to harassment or stalking. If so, this suggests that the potential of the law to protect individuals from online abuse is not being used to the full,[7] meaning victims are often let down.

The following section will suggest a new Bill, aimed at controlling inappropriate conduct aided by social media, an example of which can be located in Appendix A. In addition, it will be argued that more adequate training and education is needed within police forces, before turning to look at the CPS guidelines on prosecuting cases involving communications sent *via* social media (the guidelines).

The Criminal Justice System: The Social Media Bill

[5] Caroline Criado-Perez, ‘A Brief Comment on Peter Nunn, Sentenced Today For Twitter Abuse’ (*Week Women*, 2014) <https://weekwoman.wordpress.com/2014/09/29/a-brief-comment-on-peter-nunn/> accessed 29 October 2016
[6] *R v Peter Nunn* The City of London Magistrates Court 29 September 2014 (unreported)
[7] Similar arguments have been raised regarding revenge pornography. See, Ben Robinson & Nicola Dowling, ‘Revenge porn laws “not working”, says victims group’ *The BBC* (London, 19 May 2019) <https://www.bbc.co.uk/news/uk-48309752> accessed 26 June 2019

The purpose of the Social Media Bill will be to protect individuals from abusive and oppressing behaviour aided by new technology. By creating a coherent framework of social media related offences, the Bill will act as a form of deterrence for future online conduct. It codifies, consolidates, and creates new substantive offences which can be aided by new technology, creating strong legal provisions which both protects citizens from online abuse, whilst also deterring individuals from taking part in inappropriate behaviour online. The Social Media Bill will take precedence in matters relating to digital media, as opposed to the current use of adapting and shaping Acts of Parliament never intended to govern online conduct. This in turn creates provisions better suited to a digital age.

Unlike many of the current legal provisions contained in the legal system of England and Wales, the Social Media Bill has been created specifically with new technology in mind. Though the Bill will mainly cover social media, to ensure the Bill keeps pace with the changing nature of technology the Social Media Bill does not contain a specific definition of social media. Instead, the Bill uses the term 'technology' which is defined as 'a device for storing, processing and retrieving information'.[8] This allows some form of flexibility within the law, without breaching the fundamental principle of legality in the criminal law. As potently put by Lord Bingham:

> 'It is accepted that absolute certainty is unattainable, and might entail excessive rigidity since the law must be able to keep pace with changing circumstances, some degree of vagueness is inevitable ...'.[9]

[8] *Director of Public Prosecutions v McKeown* [1997] 1 W.L.R. 295 per Lord Hoffman 302
[9] *R v Rimmington, R v Goldstein* [2005] UKHL 63, [2006] 1 A.C. 459 per Lord Bingham [35]

By creating strong legal provisions suited to a digital age the Bill will not only conform to freedom of speech, it will in turn protect a person's right to privacy. As highlighted in chapter seven the criminal justice system currently tilts in the direction of freedom of expression. By strengthening the law's surrounding online abuse, a person's right to physical and psychological integrity will be more adequately protected.

To protect freedom of expression, in many of the provisions contained under the Act reference is made to 'reasonable members of society'. Here, reasonable members of society will be considered the reasonable social media user as endorsed by the UK Supreme Court in *Stoker v Stoker*:[10]

> 'The touchstone remains what would the ordinary reasonable reader consider the words to mean … All of this, of course, emphasises that the primary role of the court is to focus on how the ordinary reasonable reader would construe the words. And this highlights the court's duty to step aside from a lawyerly analysis and to inhabit the world of the typical reader of a Facebook post. To fulfil that obligation, the court should be particularly conscious of the context in which the statement was made …'.[11]

Here, the police, the CPS and the courts will need to take into consideration how the reasonable social media user would interpret the objectionable content, alongside any other criteria contained within the proposed Social Media Bill.

In addition, to ensure the protection of privacy, which as discussed in chapter seven entails the protection of another's physical and psychological integrity, many of the provisions put forward in the draft Social Media Bill, contain the

[10] *Stoker v Stoker* [2019] UKSC 17
[11] *Ibid.,* per Lord Kerr [37-38]

clause that the behaviour must cause another anxiety or distress. Under the Bill, utilising the judgment of the court in *Majrowski v Guy's and St Thomas's NHS Trust*[12] anxiety is defined as 'something just short of a recognised psychiatric illness'.[13] Whereas distress is defined as 'oppressive and unreasonable behaviour' based on the reasonable person.[14] This allows for the courts, the CPS and the police to be more aware of the harms associated with online abuse. Below, each provision contained in the draft Social Media Bill will be taken in turn and explained.

Cyber Harassment and Cyberstalking

Though harassment and stalking are currently criminalised under sections 2 and 2A of the Protection from Harassment Act, as discussed in chapter four there are several issues with the application of the Protection from Harassment Act in a digital age. For example, chapter four highlighted issues with a lack of clarity as to the meaning of harassment and stalking, which in turn has led to a number of failures in the criminal justice system, particularly when these behaviours are conducted *via* the use of social media. For instance, a report conducted by the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate in 2017 outlined failures by the police to truly understand the difference between harassment and stalking.[15] This is despite the White Paper suggesting that cyber harassment and

[12] *Majrowski v Guy's and St Thomas's NHS Trust* [2005] EWCA Civ 251, [2005] Q.B 848
[13] *Ibid.,* per Auld LJ [45
[14] *Ibid.,* per May LJ [82]
[15] Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate, 'Living in fear – the police and CPS response to harassment and stalking' (*justiceinspectorates.gov*, July 2017) <http://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/living-in-fear-the-police-and-cps-response-to-harassment-and-stalking.pdf> accessed 29 November 2017

cyberstalking are clearly defined.[16] The proposed Social Media Bill, located in Appendix A, has attempted to overcome this issue by specifically criminalising the conducts of cyber harassment and cyberstalking with a clear and accessible definition, whilst also removing the condition of a course of conduct.[17]

Under the Social Media Bill cyber harassment is defined as the use of technology which the reasonable person would regard as causing another anxiety or distress, in which there is an awareness on behalf of the defendant that their behaviour could cause another anxiety or distress. The *actus reus* of the offence consists of two elements. First, the person must conduct the behaviour with the aid of technology. Second, the reasonable person must consider the behaviour as causing another anxiety or distress. The use of the term 'reasonable person' mirrors provisions contained in the criminal code of Australia which prohibits the use of technology to harass, menace or send offensive content to another, as highlighted in chapter eight:

> 'A person commits an offence if: (a) the person uses a carriage service; and (b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.'[18]

[16] HM Government n.2, [2.2]
[17] As discussed in chapter four in order to prove harassment, the Protection from Harassment Act 1997 states that contact must occur between the defendant and the victim on at least two occasions over a reasonable period of time, known as a course of conduct. See, the Protection from Harassment Act 1999 7(3)
[18] Criminal Code Act (1995) section 474.17(1) (Australia)

Not only does the inclusion of the term 'reasonable person' in both the Australian Criminal Code and the proposed Social Media Bill protect freedom of expression it also, as potently put by Plater:

> '… allows for community standards and common sense to be considered when determining whether certain conduct or content of a communication is menacing, harassing or of an offensive nature.'[19]

Whereas, the *mens rea* of the offence contained in the Social Media Bill is based on the construction of knowledge. Here, the defendant needs to know, or ought to know, that their behaviour would cause another anxiety or distress, mirroring the *mens rea* of harassment contained in section 1 of the Protection from Harassment Act.

The Social Media Bill goes on to specifically criminalise cyberstalking. Like that of cyber harassment, the conduct of cyberstalking must be conducted with the aid of technology, in which the reasonable social media user would regard the conduct as amounting to the anxiety or distress of another. In addition, to separate cyberstalking from cyber harassment the conduct must 'be considered as continued unwanted contact', removing the minimum requirement set out by Parliament under the Protection from Harassment Act. Like cyber harassment, the *mens rea* of the offence is based on the construction of knowledge, whereby the defendant must know or ought to know that their behaviour could cause another anxiety or distress.

[19] David Plater, '"Setting the boundaries of acceptable behaviour?" South Australia's latest legislative response to revenge pornography' (2016) 2 UniSA Student Law Review 77, 82

The behaviours of cyber harassment and cyberstalking can have a significant effect on a person's wellbeing, as highlighted at various points in this thesis. It has given rise to not only victims changing their online habits, but it has also resulted in devastating consequences for those who have become subjected to this form of abuse. By directly placing cyber harassment and cyberstalking on a statutory footing, it allows for the criminal justice system to better protect those who become victims of this form of abuse.

Cyber Related Revenge Pornography

Revenge pornography has been defined as the ultimate humiliation of another,[20] with it becoming a specific criminal offence in England and Wales in 2015 under section 33 of the Criminal Justice and Courts Act. As discussed in chapter five the criminalisation of revenge pornography has been hailed as a success by the CPS.[21] However, the law itself is not without fault due to the narrow nature in which the law has been constructed.[22] For instance, the definition of sexual imagery does not cover photoshopped images, the *mens rea* of the offence is one of intent, and images sent to another which are not distributed to cause distress upon the person contained in the image, will fall outside the realms of the Act.

[20] HC Deb 19 June 2014, vol 582, col 1368
[21] The Crown Prosecution Service, 'Violence against women and girls report: tenth edition' (*CPS.gov*, 2017) 1 <https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2017.pdf> accessed 30 January 2018
[22] Robinson & Dowling n.7

As outlined in Appendix A, the Social Media Bill attempts to overcome the issues highlighted in chapter five by widening the scope of section 33 of the Criminal Justice and Courts Act. Consequently, the *mens rea* of the offence has been altered to include photos or videos which are sent recklessly, mirroring the *mens rea* suggested by Mitchell as previously discussed in chapter five.[23] By extending the *mens rea* of section 33 of the Criminal Justice and Courts Act, it allows for victims of this form of abuse to be better protected by the law.

Furthermore, to satisfy the *mens rea* of the offence contained in clause 2 of the Social Media Bill, there must also be some form of knowledge on behalf of the defendant that the material being disclosed lacks consent on behalf of the person capsulated in the image or video. Like that of cyber harassment and cyberstalking, under the Social Media Bill knowledge is built on the principle that the defendant should know or ought to know that there was a lack of consent. Here, the term 'consent' includes '… general consent covering the disclosure, as well as consent to the particular disclosure.'[24] This ensures that individuals who reshare the image online may only be prosecuted if they actively know that there is a lack of consent.

The *actus reus* of the offence, like that of section 33 of the Criminal Justice and Courts Act is the disclosure of private sexual photographs or films to another. However, under the new provisions put forward in the Social Media

[23] Justine Mitchell, 'Censorship in cyberspace: closing the net on "revenge porn"' (2014) 25(8) Entertainment Law Review 283, 288
[24] The Criminal Justice and Courts Act 2015 section 33(7)a

Bill, the condition that the picture has to be sent to cause distress upon the person contained in the material, has been removed. Furthermore, in order to widen the scope of revenge porn laws the definition of 'private sexual photograph or film to another', under the Social Media Bill has been expanded to reflect the work of Mitchell.[25] Here, the term 'sexual' is defined as a person:

> 'engaged in sexual intercourse; or unclothed external genitalia, the perineum and anus of a male or female; Buttocks of a male or female; Breasts and nipples of a female; and covered erectile genitalia of a male are clearly visible; or a photo or film that the reasonable person would consider as sexually explicit'.[26]

The Social Media Bill also makes it an offence to send a 'private sexual photograph or film to another' even if the image is photoshopped. As outlined in previous chapters the advancements of changing technology means photos can be dramatically altered to the point in which the person viewing the photo may not be able to see that it is a fake image.

One of the most crucial changes put forward in clause 2 of the Social Media Bill relates to anonymity. As highlighted in chapter five one of the major criticisms of section 33 of the Criminal Justice and Courts Act relates to the lack of anonymity given to revenge porn victims.[27] Revenge porn is *akin* to a sexual offence as opposed to blackmail despite arguments to the contrary made by ex-policing minister Mike Penning.[28] Victims are left traumatised, resulting in significant mental health issues, as the law as it currently stands

[25] Mitchell n.23. See chapter five for a detailed discussion.
[26] *Ibid.,* 288
[27] Robinson & Dowling n.7
[28] Jocelyn Ledward & Jennifer Agate, '"Revenge porn" and s.33: the story so far' 28(2) Entertainment Law Review 40, 41

neglects victimological aspects of revenge porn. Consequently, the Social Media Bill, by utilising section 1(1) of the Sexual Offences (Amendment Act) 1992, gives anonymity to victims of revenge pornography to ensure they are given full protection under the law.

Online Abuse

As outlined in chapter six both sections 127 of the Communications Act and the Malicious Communications Act, can be considered as provisions criminalising miscellaneous online offences. Between these two legal provisions conduct that can be labelled as threatening, false, obscene, indecent, grossly offensive or menacing are prohibited. Indeed, in recent years both these provisions have become interchangeable within the criminal justice system.[29] Despite this, both provisions can be considered to take precedence in social media related offences. However, as discussed previously neither provision is without fault. For instance, the term grossly offensive as contained in section 127(1) of the Communications Act and within the Malicious Communications Act, has been criticised for its lack of a definitive definition.[30] In fact in India, as discussed in chapter eight provisions of the Information Technology Act 2000 have been struck down by the Indian Supreme Court as the term 'grossly offensive' was considered too vague and lacked an agreed definition.[31]

[29] Laura Scaife, *Handbook of Social Media and the Law* (Routledge 2015) 166
[30] Laura Bliss, 'The crown prosecution guidelines and grossly offensive comments: an analysis' (2017) 9(2) Journal of Media Law 173
[31] *Shreya Singhal v Union of India* (2013) 12 S.C.C. 73

Under clause 4 of the Social Media Bill as illustrated in Appendix A, it is proposed that it will be an offence to send a message or content that can be labelled as either grossly offensive or menacing *via* the use of technology. The *actus reus* of the offence consists of three elements. First, the offence must be committed using technology. As explained above technology is given a wide definition under the Bill, to ensure that the law is flexible to advancements of digital media. Second, it must be found that the reasonable person, i.e. the reasonable social media user,[32] would consider the content as contributing to the anxiety or distress of another. Finally, the conduct in question needs to amount to an offence which can be labelled as either grossly offensive or of a menacing nature.

Under the Bill menacing is defined as 'something just short of a credible threat', reflecting the definition given to the term by Sedley LJ in *Director of Public Prosecutions v Collins*.[33] Whereas grossly offensive will be defined under the Social Media Bill as something:

> 'more than offensive, shocking or disturbing; or satirical, iconoclastic or rude comment; or the expression of unpopular or unfashionable opinion about serious or trivial matters, or banter or humour, even if distasteful to some or painful to those subjected to it; or an uninhibited and ill thought out contribution to a casual conversation where participants expect a certain amount of repartee'.[34]

[32] *Stoker v Stoker* n.10
[33] *Director of Public Prosecutions v Collins* [2005] EWHC 1308 (Admin), [2006] 1 W.L.R. 308 per Sedley LJ [10]. See also, David Allen Green, 'The "Twitter Joke Trial" returns to the High Court' (*NewStatesman*, 22 June 2012) <https://www.newstatesman.com/blogs/david-allen-green/2012/06/twitter-joke-trial-david-allen-green> accessed 30 April 2018.
[34] The Crown Prosecution Service, 'Guidelines on Prosecuting Cases Involving Communications Sent via Social Media' (*CPS.gov*, 21 August 2018) [28] <https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media> accessed 11 October 2018

The inclusion of the term ‘more than’ allows for freedom of speech to be protected. Here, it will be for the criminal justice system, based on the reasonable social media user, to determine when a comment breaches the elements contained in the above definition.[35]

Providing a clearer definition of the terms grossly offensive and menacing with the aid of case law examples would ensure that the Social Media Bill adheres to the principle of legality, whilst also maintaining free speech within society. The *mens rea* of knowledge also adds further protection for freedom of speech in a digital age. The application of this provision will be aided further by updated social media prosecuting guidelines, discussed in detail in further sections of this chapter.

Clause 4 of the Social Media Bill will also directly criminalise the sending of false messages and messages sent using false credentials. As discussed in chapter six fake online profiles are becoming a prominent problem within society. These profiles are often created for the sole aim of abusing another. In fact, Twitter has no ‘real name’ policy, meaning users can create a Twitter account using false credentials. Under the Social Media Bill it will be an offence to send *via* technology, a message of a grossly offensive or menacing nature which the person knows to be false or the message is sent using a fake social media account. Like that of other provisions contained in the Social Media Bill, the *mens rea* will be based on the construction of knowledge.

[35] *Stoker v Stoker* n10

Furthermore, clause 4 proposes that it will be an offence to send a message of an obscene nature, contrary to the Obscene Publications Act 1959 and 1964. As outlined in chapter six, although section 127(1) of the Communications Act makes it an offence to send a message or material of an obscene nature, the Obscene Publications Act seems to take precedence in cases relating to obscene material. The Obscene Publications Act can be considered to conform to the principles of legality, whilst also protecting freedom of expression, as affirmed by the European Court of Human Rights.[36] It is proposed that the Obscene Publications Act will take precedence in matters relating to obscene material sent *via* the use of technology.

The final behaviour criminalised under clause 4 of the Social Media Bill relates to the use of technology to send a threat, in particular threats of a sexual nature to another. The *actus reus* of the offence contains three elements. Like that of other provisions contained in the Bill, the material must be sent *via* the use of technology, which the reasonable social media user[37] would consider as amounting to the anxiety or distress of another. The third element relates to the content of the material. Here, it must be found that the communication under review either contains a credible threat of violence or an explicit threat of rape or sexual violence. Here, the term 'explicit' will take its ordinary dictionary meaning, namely, a clear and precise threat of sexual

[36] *Handyside v United Kingdom* (1976)1 EHRR 737
[37] *Stoker v Stoker* n.10

violence, reflecting how the law currently governs extreme pornography.[38] Like that of other provisions contained in the Bill, the *mens rea* is based on the construction of knowledge.

Inciting Others

Following the 2017 General Election in the United Kingdom the then Prime Minister, Theresa May, announced plans to investigate the continued abuse of MPs during the campaign period. In December 2017 the Committee on Standards in Public Life released their report examining the intimidation of those serving in public office.[39] The report highlighted the continuing issue of dogpiling. As discussed in chapter one dogpiling is considered the behaviour of actively encouraging other online users to abuse another online. It is becoming a prevalent problem in a digital society, especially for MPs:

> 'It got so bad during the election that for much of the campaign I came off social media and didn't post anything which impacted on my ability to campaign'.[40]

The Social Media Bill therefore specifically criminalises the behaviour of dogpiling.

Under the Bill it is an offence to:

> 'intentionally incite multiple persons to target another, which D [defendant] reasonably believes will amount to the harassment of another'.[41]

[38] The Crown Prosecution Service, 'Extreme Pornography' (*CPS.gov*, 2019) <https://www.cps.gov.uk/legal-guidance/extreme-pornography> accessed 13 May 2019
[39] Committee on Standards in Public Life, *Intimidation in Public Life: A Review by the Committee on Standards in Public Life* (HC 2017-18)
[40] *Ibid.,* per Maria Caulfield MP 39
[41] Appendix A

The *actus reus* consists of several key elements. First, multiple people must incite others to target another online. Under the Bill multiple is defined as more than two people, mirroring provisions contained in section 2 of the Protection from Harassment Act. As dogpiling is *akin* to harassment the conduct must also amount to the harassment of another. Here, the definition of harassment contained in the cyber harassment provision of the Bill will be utilised. In essence, the reasonable person must conclude that the conduct amounts to the anxiety or distress of another.

Clause 5 of the Social Media Bill also makes it an offence to incite another to commit a further criminal offence governed by law. The purpose of this provision is to create a coherent and clear offence of incitement, which conforms to the principles of legality. In previous cases as outlined in chapter four, sections 44 and 46 of the Serious Crime Act have been used to govern the incitement of others to commit a further criminal offence.[42] However, the Serious Crime Act when first enacted was never intended to cover abusive conduct carried out *via* social media. Consequently, its usage can be seen not to conform with the principles of legality in the criminal law.

The Social Media Bill makes it an offence to intentionally incite another to commit a further criminal offence, which the defendant reasonably believes will result in a further criminal offence taking place. The *actus reus* of the offence is the incitement of another to commit a further criminal act. Here, the further criminal act must be governed by statute or the common law,

[42] For instance, see *R v Blackshaw* [2011] EWCA Crim 2312, [2012] 1 W.L.R. 1126

similar to that of sections 44 to 46 of the Serious Crime Act. Whereas the *mens rea* consists of two elements. First, the incitement must be done with intention. Intention as governed under *Regina Respondent v Woollin Appellant*,[43] refers to the defendants aim or purpose. The second element of the *mens rea* is one of belief. Here, it must be found that the defendant, '… in the light of all the circumstances …' reasonably believed that a further criminal offence would take place.[44]

Hate Crime

Anyone can become a victim of online abuse though there are growing concerns surrounding the use of the Internet to target another because of a protected characteristic.[45] For instance, targeting someone because of their race or sexuality. In fact, in recent years there has been an increase in the use of social media sites to subject women to gender-specific threats of rape.[46] The Social Media Bill will contain a direct provision in which the police, the CPS and the courts must consider if any of the behaviours contained in the Social Media Bill are conducted because of someone's protected characteristic. However, to reflect the changing nature of society a wide definition will be given to the term protected characteristic:

> 'protected characteristic covers the following: race; ethnicity; national origin; religious affiliation; sexual orientation; caste; sex; gender or gender identity; or disability.'[47]

---

[43] *Regina Respondent v Woollin Appellant* [1998] 3 W.L.R. 382, [1999] 1 A.C. 82 per Lord Steyn 93
[44] *R v Edward Leonard* Hall (1985) 81 Cr. App. R. 260 per Boreham J 264
[45] The BBC, 'Hate crime "police priority" as social media cases soar' *The BBC* (London, 17 March 2018) <https://www.bbc.co.uk/news/uk-scotland-glasgow-west-43436900> accessed 19 July 2019
[46] Amnesty International UK, 'Online abuse of women widespread in UK' (*Amnesty International*, 2017) <https://www.amnesty.org.uk/online-abuse-women-widespread> accessed 3 October 2018
[47] Appendix A

Computer Misuse

The final provision contained in the Social Media Bill relates to computer misuse. As discussed in chapter five, though it is rare, computer misuse can and has been used to abuse others online.[48] However, unlike many other Acts analysed throughout this thesis, the Computer Misuse Act can be considered as conforming to the principle of legality. Consequently, clause 7 contained in the Social Media Bill ensures that in matters relating to computer misuse, the Computer Misuse Act is utilised.

Section Overview

The Social Media Bill attempts to strengthen the criminal law framework in matters relating to inappropriate behaviours online. However, to ensure consistency changes are needed across the criminal justice system including, digital media training for police officers, alongside updated and transparent social media guidelines.

The Criminal Justice System: The Police

In recent years, the police in England and Wales have witnessed a dramatic increase in reports relating to malicious communications sent online. As outlined in chapter one in 2017 the BBC released a Freedom of Information request, highlighting the number of police reports generated during 2015 and 2016 concerning online malicious communications.[49] In 2015, 33,462 reports

[48] *R v Crosskey* [2012] EWCA Crim 1645, [2013] 1 Cr. App. R. (S.) 76
[49] The BBC, 'Teenager's life "ruined" by Live.me and Twitter "trolls"' *The BBC* (London, 24 October 2017) <http://www.bbc.co.uk/news/uk-england-41693437> accessed 30 January

were made to thirty-eight out of forty-three police forces in England and Wales relating to malicious communications. By 2016 this figure had increased to 76,372 police reports.[50] However, examples have been illustrated throughout this thesis of the police failing to take reports of online abuse seriously, encouraging a victim-blaming orthodox in some instances.

A report undertaken by the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate in 2017 as discussed in detail in chapter four, exposed a lack of understanding across the criminal justice system in relation to harassment and stalking offences.[51] In particular, concerns were raised regarding the criminal justice systems approach to stalking and harassment in an online context:

> 'Basically they've told me [the police], any contact that I receive through social media is irrelevant, because they can't prove that it's associated to them [the abuser].'[52]

Throughout the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate report, examples are given of failures by both the police and the CPS in adequately protecting those who are subjected to harassment or stalking. Social media has in recent years changed how harassment and stalking can be carried out. For instance, of the 112 reports examined by the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate, 82 cases involved the use of modern technology, such

2018. Here, the term 'malicious communication' was used as a generic term for abusive commentary sent online

[50] *Ibid.,*

[51] Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate n.15

[52] *Ibid.,* 27

as social media, by the perpetrator to carry out the offence.[53] Failure by the police in taking online abuse seriously can have serious consequences.

In 2017 Molly McLaren was stabbed 75 times outside a gym by her ex-partner.[54] Ms McLaren had previously ended her relationship with Joshua Stimpson over concerns about his controlling behaviour. He proceeded to harass her *via* Facebook.[55] She reported Stimpson's behaviour to her local police force stating that he had 'lost the plot' and she was in fear of her own life.[56] Despite these concerns Stimpson simply received a phone call from a police officer, warning him about his behaviour. A week after the phone call Stimpson killed Ms McLaren resulting in Kent Police force referring themselves to the Independent Office for Police Misconduct.[57]

From the examples given above and throughout this thesis, more adequate training is needed for police officers relating to the use of social media to commit unlawful behaviour.[58] Training however needs to go beyond establishing when certain conduct crosses the line to warrant criminal law intervention; it needs to include a better understanding across police forces with regard to how social media websites work, how to adequately support victims who are being subjected to online abuse, tackle the stigma that

---

[53] *Ibid.,* 52
[54] Sarah Ditum, 'If the law actually worked, Joshua Stimpson wouldn't have been able to stab Molly McLaren 75 times in broad daylight' *The Independent* (London,7 February 2018) <https://www.independent.co.uk/voices/molly-mclaren-stalking-joshua-stimpson-stabbed-theodore-johnson-cps-a8198836.html> accessed 3 April 2019
[55] Laura Bliss, 'The Protection from Harassment Act 1997: Failures by the Criminal Justice System in a Social Media Age' (2019) 83(3) Journal of Criminal Law 217, 226
[56] *Ibid.,*
[57] As of 16 April 2019, The Independent Office for Police Misconduct were still investigating the matter.
[58] Robinson & Dowling n.7

online abuse is outside the realms of the 'real world', and updated training in relation to major technological changes or advancements.

The approach that social media is beyond the scope of the legal system has now been eroded. In England and Wales nearly half of all crime is aided by social media.[59] Police officers need to be adequately trained in the advancements of changing technology. The Home Office in 2016 announced plans to invest in the education of law enforcement. As part of a £4.6 million Police Transformation fund programmes will be created to help '… build police capability to respond to the full range of digital crime types, through investment in technology and training.'[60] However, for training to be successful police forces need to be aided by up-to-date social media prosecuting guidelines which are explicit and clear.

The Criminal Justice System: The Crown Prosecution Service Guidelines

Following growing concerns about the lack of consistency between police forces in matters relating to social media;[61] the matter of Paul Chambers, an individual prosecuted for the sending of a tweet threatening to blow an airport 'sky high';[62] and the case of Daniel Thomas, a footballer who sent a

[59] Kate McCann, 'Social media giants should be forced to pay for policing social media, report backed by Amber Rudd claims' *The Telegraph* (London, 1 May 2017) <https://www.telegraph.co.uk/news/2017/04/30/social-media-giants-should-forced-pay-policing-social-media/> accessed 24 January 2019
[60] HM Government n.2, [1.16]
[61] Bliss n.30, 174
[62] *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin), [2013] 1 WLR 183

homophobic tweet about the divers Tom Daley and Peter Waterfield,[63] the CPS announced plans to implement prosecuting guidelines on social media offences. As discussed in detail in chapter six the guidelines were introduced in 2013, later being updated in 2016 and 2018. The purpose of the guidelines was to provide clear advice for prosecutors and the police in cases relating to inappropriate behaviour carried out *via* social media.[64] However, as exposed in chapter six there have been several issues in the application of the guidelines to cases of online abuse.

Alison Chabloz in 2018 was successfully convicted under section 127(1) of the Communications Act for the sending of grossly offensive, obscene or menacing messages relating to the Holocaust.[65] Yet as outlined in chapter six the original case before the courts was brought by a private prosecution, following a failure by the police and the CPS to take legal action against Chabloz; providing a prime example of the lack of consistency still present in the criminal justice system, despite social media prosecuting guidelines being in place. Furthermore, following the implementation of the guidelines and subsequent updates, fewer recommendations for prosecutions were put forward by the CPS.[66]

[63] The Crown Prosecution News Brief, 'DPP Statement on Tom Daley Case and Social Media Prosecutions' (*CPS.gov,* 2012) <http://blog.cps.gov.uk/2012/09/dpp-statement-on-tom-daley-case-and-socialmedia-prosecutions.html> accessed 29 April 2018
[64] The Crown Prosecution Service, 'Guidelines on Prosecuting Cases Involving Communications Sent via Social Media' (*CPS.gov*, 2013) <http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_ media/index.html> accessed 27 February 2016
[65] *R v Alison Chabloz* Westminster Magistrates' Court 25 May 2018 (unreported)
[66] See figure six chapter six

Throughout the guidelines significant reference is made to freedom of expression with very little reference to privacy. As discussed in chapter seven freedom of expression is an important aspect of a democracy and needs to be taken into consideration, but this should not be at the expense of privacy. Privacy is more than a person's right to a life away from the public realm, it is a right not to have ones physical or psychological integrity attacked.[67] Here, the CPS guidelines should endorse the approach of the House of Lords in *Campbell v MGN Ltd*[68] where the concept of privacy was examined first, before turning to look at freedom of expression:

> '… [the] question is whether the objective of the restriction on the article 10 right - the protection of [Ms] Campbell's right under article 8 to respect for her private life - is sufficiently important to justify limiting the fundamental right to freedom of expression …'.[69]

In essence, the guidelines need to encourage prosecutors and the police to take into account the victims right to privacy before that of the perpetrators right to freedom of expression.

The balance between freedom of expression and the right to privacy is not unique to the digital age, it has always existed with traditional forms of media. However, social media has dramatically changed behaviours commonly associated with the physical world such as bullying, stalking and harassment. These behaviours can now be aided or solely conducted *via* social media and often occur around the clock.[70] The CPS guidelines should be updated regularly to include case examples which clearly highlight the

[67] *Pfeifer v Austria App* no 125561/03 [2007] ECTHR 935 [33]
[68] *Campbell v MGN Limited* [2004] UKHL 22
[69] *Ibid.,* per Lord Hope of Craighead [113]
[70] Neil MacEwan, 'The new stalking offences in English law: will they provide effective protection from cyberstalking?' (2012) 10 Criminal Law Review 767, 771

decisions of the CPS and the courts. So, for instance include examples of cases which were deemed worthy of prosecution, highlighting why this decision was made alongside the judgment of the court. In addition, cases which were not put forward for prosecution should be included to ensure transparency.

The CPS guidelines on social media prosecutions were a significant step forward in helping to tackle the growing issue of online abuse, but they are far from perfect, as highlighted in the recent Law Commission's report into online behaviours.[71] Nevertheless, it is accepted that in order to help tackle online abuse, changes outside the criminal justice system also need to be strengthened, creating a multidimensional approach to tackling online abuse.

Education[72]

Education is an important tool in creating a safe online environment for all Internet users. As outlined in chapter eight the Federal Government of Australia believes that education is '… one of the most important elements of crime prevention',[73] an approach that needs to be mirrored on a global scale. Indeed:

> '[c]hildren have also told us [the Government] that they want more education about online safety, as well as more support from tech

[71] Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018) [4.147]
[72] Education in the United Kingdom is a devolved issue between England, Scotland, Wales and Northern Ireland. In this section reference is made to changes put forward by the Department of Education who oversee the education of the younger generation in England. However, the recommendations put forward in this section should be implemented across the whole of the United Kingdom, including schools which are not run by the State.
[73] Parliament of Australia, *Cyber Safety - Joint Select Committee High-wire act: Cyber-safety and the young Interim report* (June 2011) [11.18]

companies to keep them safe.'[74]

Education needs to take a two-dimensional approach. First, better education is needed within schools relating to the online world. Second, parents also need to be educated to ensure they fully understand the implications of inappropriate behaviour online.

Education: Children

Technology has had a significant impact on educational institutions across the globe.[75] We are now living within a society where some generations do not know a world without the Internet, or indeed social media. Yet in England compulsory computer education is only just starting to be implemented within state-based schools[76] to ensure:

> 'all young people are equipped to have healthy and respectful relationships in both the online and offline world, and leave school with the knowledge to prepare them for adult life.'[77]

Though this is a significant step forward the Internet has been part of mainstream society since the turn of the millennium. Consequently, the United Kingdom's Government is wanting to implement more adequate computer-based education within Primary and Secondary schools.

[74] HM Government n.74, [9.3]
[75] George Veletsianos 'The Defining Characteristics of Emerging Technologies and Emerging Practises in Digital Education' in George Veletsianos (ed), *Emergence and Innovation in Digital Learning: Foundations and Applications* (Athabasca University Press 2016) 10
[76] As previously noted throughout the UK, there are several ways in which schools are funded. Those not run by the state do not always have to follow the changes implemented by the Government.
[77] HM Government, n.1

The education of the younger generation is built on three interlocking pillars: reading, writing and mathematics.[78] These three subjects are considered the foundation of the educational system in which all students should leave school knowing how to read, write and have a basic understanding of arithmetic. In recent years there has been a drive to add a fourth pillar: Digital Literacy.[79] Digital Literacy is:

> '[t]he social and emotional literacy and digital competency to positively respond to and deal with any risks they might be exposed to when they [online users] are using social media or going online'.[80]

In essence, Digital Literacy will encompass educating all students on all aspects of the digital world, from how to use technology to behaviours which are unacceptable online such as cyberbullying.

Currently, under the new computer curriculum students are taught basic computer skills such as word processing, spreadsheets and how to use search engines.[81] Whereas schools that endorse a Digital Literacy approach will ensure that students are educated about the dangers of the online world, including how to spot online dangers, encourage students to think critically about the content they are exposed to, understand that actions conducted online have real-life consequences, and help to build online resilience.[82]

---

[78] Select Committee on Communications, *Growing up with the internet* (HL 2016-17, 130) 4
[79] *Ibid.,*
[80] Young Minds, 'Resilience for the digital world' (*Young Minds*, January 2016) <https://youngminds.org.uk/assets/0002/6859/Resilience_for_the_Digital_World_YM_Positioning.pdf> accessed 21 March 2019
[81] HM Government n.1, 26
[82] *Ibid.,*

The Department of Education, which oversees the curriculum in schools in England, is due to publish an Education Technology strategy in late 2019. The purpose of the strategy will be to provide clear guidance to schools and colleges to support the implementation of Digital Literacy within the school curriculum.[83] Furthermore, the UK Government has funded a UK Safer Internet Centre to aid schools in providing online safety toolkits and updated guidance on cyberbullying.[84] However, presently, Digital Literacy is not compulsory across all schools, leaving in many cases not-for-profit organisations to educate the younger generation about online safety.[85]

Digital Literacy is an important aspect in helping to tackle inappropriate behaviour online. In the UK alone 99% of 12 to 15 year olds use the Internet regularly.[86] The Government's White Paper endorses a number of principles which will underpin Digital Literacy lessons, including:

> '[e]nsuring that users can be more resilient in dealing with mis- and disinformation, including in relation to democratic processes and representation; [e]quipping people to recognise and deal with a range of deceptive and malicious behaviours online, including catfishing, grooming and extremism; [e]nsuring people with disabilities are not excluded from digital literacy education and support; [and] [d]eveloping media literacy approaches to tackling violence against women and girls online.'[87]

By educating the younger generation the foundations for a safer online world are created, where individuals can understand the ethical, social and criminal implications of their behaviour online.

---

[83] HM Government n.2, [8.17]
[84] *Ibid.,* [9.10]
[85] For instance, Online Media UK. See, Dr Holly Powell-Jones, 'Online Social Media: Law and Ethics' (*Online Media Law UK*, 2019) <https://cml.sad.ukrd.com/document/612785.pdf> accessed 21 March 2019
[86] HM Government n.2
[87] *Ibid.*, [9.19]

To financially support Digital Literacy Skills workshops, the United Kingdom's Government has proposed to implement a social media levy:

> 'Some companies have already invested heavily to improve the online safety of their users, including through supporting end-user and civil society groups. However, we [UK Government] believe that more needs to be done and that it is right that all companies should be involved and encouraged to play their part. This is the reason we [UK Government] will introduce a levy, to help us combat online harms.'[88]

The purpose of the levy is to help with the costs of educating sectors of society about online harms. However, social media companies will not be obliged to contribute to the levy as it will be a voluntary payment, like the voluntary levy contained in section 10C of the Gambling Act 2005.

Under the Gambling Act the Secretary of State has created regulations to impose a voluntary annual payment on organisations who hold licenses issued by the Gambling Commission.[89] In essence, each year organisations, such as Highstreet Bookmakers make a voluntary payment to the Gambling Commission. These funds are then used to aid charity organisations such as GambleAware, who support those with gambling addictions. The voluntary payment by the gambling industry has been a success. For instance, between 2015 and 2016 GambleAware was issued with £8.1 million to help with not only the costs of educating the public but also to help provide treatments for gambling addicts.[90]

[88] HM Government n.1, 16
[89] Gambling Act 2005 section 10C 1
[90] HM Government n.1, 17

The Government anticipates that the success of the gambling levy can be mirrored in the creation of a social media levy. In the first quarter of 2018 Facebook generated $11.97 billion in revenue, despite negative press reports surrounding the Cambridge Analytica Scandal, in which it emerged that 87 billion Facebook users had their data harvested by a third party.[91] The social media levy will be used to help create educational schemes across the United Kingdom aimed at promoting online safety, educate social media users on the harms associated with online abuse, and help to provide support for those who are subjected to abuse online.

Education: Parents

Parental guardians are now more concerned about the safety of their children online than smoking or drinking.[92] We live in a society dominated by an 'always on' culture where bullying now emerges outside the context of the school environment:

> 'We have talked to young people who describe the distress they face in the playground because people are calling them names. That distress follows them on to their Facebook page, and it follows them on to their WhatsApp group among all their friends. Suddenly, it is as if they are always being seen; they cannot hide from that abuse. It is important to recognise that, because the constant surveillance means they feel that they are constantly under threat.'[93]

[91] Olivia Solon, 'Facebook posts record revenues for first quarter despite privacy scandal' *The Guardian* (London, 25 April 2018) <https://www.theguardian.com/technology/2018/apr/25/facebook-first-quarter-2018-revenues-zuckerberg> accessed 27 March 2019

[92] Personal, Social, Health and Economic Association, 'Parents call for education to address sexting by children and young people' (*PSHE Association*, 20 July 2016) <https://www.pshe-association.org.uk/news/parents-call-education-address-sexting-children> accessed 25 March 2019

[93] Select Committee on Communications n.78, [118]

The dominance of the Internet, in particular social media means that parents need to fully understand not only how the Internet works, but the safety mechanisms that can be employed to better protect their children.

Like that of the younger generation, in recent years there has been a move towards educating the older generation about online safety.[94] Local libraries often run computer-based skills workshops but funding cuts across the country are putting these workshops at risk.[95] To combat the discrepancies in children and adult Digital Literacy skills, the Government has announced plans for parents and carers with children in primary schools to receive online safety guidance.[96] This will allow parents to get a better understanding of the online world from an early stage, rather than waiting until the issue directly affects them. As outlined by the Communications Committee parents need clear guidance on social media usage.[97]

In early 2019 stories started to emerge online concerning a puppet who supposedly appeared during videos uploaded onto the social media site YouTube.[98] Allegedly, the puppet Momo, would encourage users to partake in dangerous activities such as self-harm and asphyxiation, known as the Momo challenge. Following the increasing reports online concerning Momo,

[94] HM Government n.1, 32
[95] Sian Cain, 'Nearly 130 public libraries closed across Britain in the last year' *The Guardian* (London, 7 December 2018) <https://www.theguardian.com/books/2018/dec/07/nearly-130-public-libraries-closed-across-britain-in-the-last-year> accessed 25 March 2019
[96] HM Government n.1, 27-28
[97] Communications Committee, *Regulating in a digital world* (HL 2017-19, 299) 62
[98] Phoebe Southworth, 'Parents warned about 'Momo' suicide game on YouTube' *The Telegraph* (London, 27 February 2019) <https://www.telegraph.co.uk/news/2019/02/27/parents-warned-online-suicide-game-appearing-peppa-pig-videos/> accessed 25 March 2019

which quickly caught the media's attention, parents across the country panicked with many choosing to limit their child's technology intake and schools issuing warnings to parents.[99] Though the Momo challenge was later proven to be a hoax, it illustrated the need to educate the wider public on online safety.[100]

The Government has announced that it will continue to support parents in helping to prevent and deal with harms associated with the online world.[101] Education is an important aspect in tackling online abuse. By educating online user's issues such as online safety and how to conduct oneself online can be strengthened. This in turn can allow users to understand the real-life implications online abuse can have on another person, such as the detrimental psychological effects that can occur, as discussed in chapter one and seven**.** Yet it is not just for schools and parents to educate online users, social media companies also need to help educate their users by ensuring that education and advice become integrated into the online experience.[102]

Gatekeepers

The dominance of social media today means that companies such as Facebook and Twitter need to do more to help restrict unlawful behaviour and abuse that continues to be a problem on their sites. Though Facebook

[99] *Ibid.,*
[100] Keza MacDonald, 'Parents: don't panic about Momo - worry about YouTube Kids instead' *The Guardian* (London, 28 February 2019) <https://www.theguardian.com/commentisfree/2019/feb/28/parents-momo-scare-youtube-kids> accessed 25 March 2019
[101] HM Government n.2, [9.15]
[102] Communications Committee n.97, 62

and Twitter are continuing to strengthen their terms of service agreements and implement new systems to tackle inappropriate behaviour online, as exposed in chapter three, issues remain. For instance, Artificial Intelligence (AI) technology is currently inadequate when it comes to highlighting hate-related speech, there is a lack of legal repercussions for social media sites, and inconsistencies across social media platforms with regards to what content is or is not acceptable online. The following discussion will outline how social media companies can do more to control inappropriate behaviours on their sites, in particular looking at the advancements of AI technology and the implementation of a universal code of conduct.[103]

Gatekeepers: AI Technology

AI Technology is considered by Facebook founder and CEO Mark Zuckerberg, as one of the '… greatest opportunities to keep people safe' online.[104] AI technology encompasses computer algorithm programmes to search for certain content on a given website or platform. So, for instance in relation to social media, it can be used to find certain content that contains a specific word or hashtag. This allows for social media companies to locate unlawful or abusive behaviour before it becomes publicly viewable.

Following a Terrorist attack in Christchurch New Zealand, social media companies employed AI technology to locate and remove a video taken by the perpetrator of the offence, which was being actively shared across social

[103] A draft Universal Code of Conduct is located in Appendix B.
[104] Mark Zuckerberg, 'Building Global Community' (*Facebook*, 16 February 2017) <https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/> accessed 14 January 2019

media sites.[105] The original video which was livestreamed[106] on Facebook was removed an hour after the event occurred.[107] However, other Facebook users reuploaded the video across social media sites. In the first 24 hours after the Christchurch attack, Facebook removed 1.5 million copies of the video from its site, with the aid of AI technology.[108] Of this, in 1.2 million instances AI technology allowed Facebook to block users from uploading the video before it became publicly viewable.[109] However, a further 300,000 videos were actively removed from Facebook by moderators after they had been made publicly available, which had not been flagged by AI technology.[110]

AI technology is a significant tool in helping to combat unlawful behaviour online, but as the events surrounding the Christchurch attack illustrated, it is far from perfect. The Government in their Internet Safety Strategy uphold the ideal that the best solutions to keep individuals safe online involve technology, but more needs to be done to encourage social media companies to work faster at advancing AI technology.[111] This has been further endorsed in the White Paper:

---

[105] The BBC, 'Facebook: New Zealand attack video viewed 4,000 times' *The BBC* (London, 19 March 2019) <https://www.bbc.co.uk/news/business-47620519> accessed 26 March 2019

[106] Livestreamed technology allows for online users to video share with other internet users live. See, Facebook, 'Going Live on Facebook' (*Facebook*, 2019) <https://live.fb.com/about/> accessed 26 March 2019

[107] Jim Waterson, 'Facebook removed 1.5m videos of New Zealand terror attack in first 24 hours' *The Guardian* (London, 17 March 2019) <https://www.theguardian.com/world/2019/mar/17/facebook-removed-15m-videos-new-zealand-terror-attack> accessed 26 March 2019

[108] *Ibid.,*

[109] *Ibid.,*

[110] *Ibid.,*

[111] HM Government n.1, 20 See also, Committee on Standards in Public Life n.39, 14

> ‘Technology can play a crucial role in keeping users safe online. By designing safer and more secure online products and services, the tech sector can equip all companies and users with better tools to tackle online harms.’[112]

In essence, social media companies would be under an obligation to invest in digital technology to help control unlawful content on their sites. Endorsing a proactive rather than a reactive approach, similar to approaches recommended by the European Union (EU).

As discussed in chapter eight social media companies are currently given specific protection under Article 14(1) of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 (the directive):

> ‘Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service …’.

Furthermore, under Article 15(1) of the directive information society services such as Facebook and Twitter, are not under a legal obligation to ‘… monitor the information which they transmit’ across their sites. Social media companies under current EU provisions are not obliged to actively seek out unlawful content published on their sites, as affirmed in *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*.[113]

The directive gives significant protection to social media companies. The directive itself was implemented into the legal system of the EU nearly 20 years ago, before two of the biggest social media sites today, Facebook and

[112] HM Government n.2, [8.1]
[113] C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECLI 771

Twitter were made available to the public. As outlined in chapter one social media dominates societies across the globe. Facebook in the UK alone has 32.6 million active users.[114] On average around 500 million tweets are sent each day *via* Twitter.[115] Consequently, the directive can be considered outdated in comparison with the advancements of technology:

> 'The e-Commerce Directive was introduced in what now feels like a bygone era … One of the biggest winners … has been the online platforms. They can provide services to millions of people worldwide, harvest their data and make millions in revenue, and yet have zero responsibility for what their customers see and experience and the harm they suffer whilst under their care. Yes, the platforms have to remove illegal content once they are notified, but they have no obligation proactively to stop that content from reaching our eyes and ears, even if they know their sites are full of it.'[116]

Nonetheless, in March 2019 the European Parliament voted in favour of implementing new copyright laws, which have been considered as revolutionising Internet governance.[117] Under these new legal provisions, tech companies will be held responsible for copyright material posted on their sites, removing the host rather than publisher defence in relation to content that breaches copyright regulations.[118] The controversial changes, which have been heavily criticised by tech companies such as Google and YouTube,[119] is the first step in ensuring tech companies are held to account

---

[114] Mark Sweney, 'Is Facebook for old people? Over-55s flock in as the young leave' *The Guardian* (London, 12 February 2018) <https://www.theguardian.com/technology/2018/feb/12/is-facebook-for-old-people-over-55s-flock-in-as-the-young-leave> accessed 29 November 2018

[115] Ursula Smartt, *Media & Entertainment Law* (Taylor & Francis 2017) 79

[116] Communications Committee n.97, 186

[117] Zoe Kleinman, 'Article 13: Memes exempt as EU backs controversial copyright law' *The BBC* (London, 26 March 2019) <https://www.bbc.co.uk/news/technology-47708144> accessed 27 March 2019. See also, Chris Fox, 'What is Article 13? The EU's copyright directive explained' *The BBC* (London, 14 February 2019)

[118] Article 13 Directive on Copyright in the Digital Single Market 2016/0280

[119] Kleinman n,117. See also, Chris Fox, 'What is Article 13? The EU's copyright directive explained' *The BBC* (London, 14 February 2019) <https://www.bbc.co.uk/news/technology-47239600> accessed 27 March 2019

for conduct that occurs across their sites. Though the host rather than publisher defence remains in relation to online abuse, this could be the first step in ensuring better online governance.

Gatekeepers: Universal Codes of Conduct

All social media companies have terms of service agreements between themselves and their users. These agreements detail what behaviour is, and is not, acceptable on a given site. Failure on behalf of users to comply with a company's terms of service agreement can result in the user being denied access to the site. However, as outlined in chapter three issues have been raised with the compliance of users to adhere to terms of service agreements, social media companies not enforcing their terms of service agreements and a lack of consistency across social media companies with regards to behaviours which are prohibited on their sites. So, for instance Twitter allows users to use online aliases to set up their Twitter account, whereas Facebook has a real name policy.[120]

Different forms of universal codes of practices exist across the globe. For example, as outlined in chapter eight the European Commission has created and implemented a code of conduct specifically aimed at some of the largest technology services across the world, defined by the European Commission as the 'IT companies'. The IT companies are under an obligation to remove unlawful content from their sites within 24 hours, though there are no legal

[120] Facebook, 'What names are allowed on Facebook?' (*Facebook,* 2019) <https://www.facebook.com/help/112146705538576?helpref=faq_content> accessed 22 April 2019

repercussions for failure to do so. Similarly, following the publication of the UK's Internet Safety Strategy and the implementation of the Digital Economy Act 2017, the United Kingdom's Government has endorsed the use of a digital code of conduct aimed at social media companies to tackle inappropriate behaviour online.

In April 2019 the Secretary of State published the UK's first digital code of conduct, in line with the publication of the White Paper. Essentially, the digital code of conduct contains four overlapping provisions which all social media providers must adhere to, or face possible fines:[121]

- Clear and accessible reporting processes to flag harmful material;
- An efficient process to update users who report unlawful content;
- Contained in the terms of service agreement should be clear and accessible mechanisms to report harmful content; and
- Clear information to users and the wider public about the actions undertaken in relation to harmful material that has been reported.[122]

The provisions contained in the digital code of conduct relate to social media companies being more transparent about how they deal with harmful content on their sites, as opposed to a specific code of conduct aimed at helping to reduce inappropriate behaviour online. However, the Government maintains

[121] HM Government n.2, [19]
[122] Department of Digital, Culture, Media and Sport, 'Code of Practice for providers of online social media platforms' (*Gov.uk*, 12 April 2019) <https://www.gov.uk/government/publications/code-of-practice-for-providers-of-online-social-media-platforms/code-of-practice-for-providers-of-online-social-media-platforms> accessed 22 April 2019

in their White Paper that a more precise code of conduct will be produced for unlawful content on social media sites such as terrorism and child abuse.[123]

From discussions throughout this thesis more needs to be done to tackle online abuse. It is proposed that a universal code of conduct should be created, alongside social media terms of service user agreements to ensure consistency across social media platforms in tackling online abuse. Whereas the digital code of conduct produced by the Secretary of State is aimed at ensuring social media providers are transparent, the proposed universal code of conduct as located in Appendix B is aimed at creating more specific obligations that all social media companies must adhere to. As noted by Williams, a lack of suitable guardians encourages criminal behaviour.[124] So, for instance the proposed universal code of conduct places an obligation on social media sites to produce terms of service agreements which are clear and accessible for all users.

As highlighted in chapter three Facebook and Twitter's terms of service agreements are at points ambiguous.[125] The ambiguity of terms of service agreements was clearly illustrated in a report conducted by the UK's Children's Commissioner in January 2017.[126] As part of a House of Lords investigation into digital media and young people, the Children's

[123] HM Government n.2, [1.28]
[124] Katherine S. Williams, *Textbook on Criminology* (7th edn, Oxford University Press 2012) 312
[125] Communications Committee n.97, 108
[126] Children's Commissioner, 'Growing Up Digital: A reports of the Growing Up Digital Taskforce' (*Children's Commissioner,* January 2017) <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf> accessed 26 March 2019

Commissioner directed a law firm to rewrite part of the terms of service agreement for the social media site Instagram,[127] to highlight the lack of clarity contained within the document. For instance, Instagram's terms of service agreement states:

> 'We do not claim ownership of your content, but you grant us a license to use it … Instead, when you share, post, or upload content that is covered by intellectual property rights (like photos or videos) on or in connection with our Service, you hereby grant to us a non-exclusive, royalty-free, transferable, sub-licensable, worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings).'[128]

When written into simplistic terminology the above term can be translated as:

> 'Officially you own any original pictures and videos you post, but we are allowed to use them, and we can let others use them as well, anywhere around the world. Other people might pay us to use them and we will not pay you for that.'[129]

Consequently, social media companies under the proposed universal code of conduct put forward in this thesis would need to ensure that all their terms are accessible and clear. In turn, this will aid moderators when reviewing flagged content.

The provisional code of conduct places further obligations on social media companies to directly tackle unlawful behaviour on their sites, with particular reference given to prohibiting hate speech, revenge pornography, trolling, bullying and threats of a sexual nature. Social media companies must, under the universal code of conduct, be more proactive in reducing and removing online abuse. Though the proposed universal code of conduct can be

[127] Note, Instagram is owned by Facebook.
[128] Instagram, 'Terms of Use' (*Instagram*, 2016) <https://help.instagram.com/581066165581870> accessed 26 March 2019
[129] Children's Commissioner n.126, 10

considered as a step forward in tackling online abuse from the current system in which social media companies have been '… allowed to mark their own homework …',[130] issues will continue to remain without a regulatory body overseeing social media companies.

Regulatory Body

Though there is some form of Internet governance in the United Kingdom, there is currently no direct regulatory body policing social media companies. Instead, social media companies have been allowed to self-regulate, which in turn has led to numerous issues in recent years. For instance, the Cambridge Analytica Scandal in 2017, the dominance of fake news, and abusive messages sent to MPs during the 2017 General Election. Consequently, arguments have emerged that a new regulatory body is needed to hold Internet based organisations to account. However, there is currently no consensus as to who should regulate social media companies. The Government's White Paper supports the concept that the Office of Communications, commonly referred to as Ofcom, should oversee the regulation of social media as outlined below. However, as discussed in later parts of this chapter it is proposed that a new regulatory body, the Digital Authority, should be created overseen by the implementation of an e-Safety Commissioner.

Regulatory Body: Ofcom

[130] Communications Committee n.97, 40

Ofcom is the United Kingdom's communications regulator and was created under the Office of Communications Act 2002, receiving their full statutory power under part one of the Communications Act. They govern several enterprises including, television, radio, video, the postal system and Internet broadband providers.[131] In addition, Ofcom has several regulatory powers under the Communications Act. For instance, setting conditions for broadcasters,[132] overseeing complaints,[133] and imposing penalties on communication providers who breach Ofcom's rules and procedures. Though Ofcom is often associated with regulating television broadcasters, Ofcom does have some statutory powers relating to the Internet.[134] However, these powers relate to Internet service providers such as British Telecom or Sky as opposed to online companies, such as social media providers.[135]

Following growing concerns relating to the dominance of social media it has been suggested that Ofcom's powers should be extended to regulate social media companies:

> 'Given the urgency of the need to address online harms, we believe that in the first instance the remit of Ofcom should be expanded … Ofcom has experience of surveying digital literacy and consumption, and experience in assessing inappropriate content and balancing it against other rights, including freedom of expression.'[136]

For the UK Government Ofcom already has the experience and expertise needed to regulate social media companies, as they already '… tackle

[131] Ofcom, 'About Ofcom' (*Ofcom*, 2019) <https://www.Ofcom.org.uk/about-Ofcom> accessed 28 March 2019
[132] Communications Act 2003 section 3
[133] Communications Act 2003 section 8
[134] Communications Act 2003 part two
[135] Ofcom, 'Phones, telecoms and internet' (*Ofcom*, 2019) <https://www.Ofcom.org.uk/phones-telecoms-and-internet> accessed 28 March 2019
[136] Communications Committee n.97, 206

harmful or offensive content, in the context of TV and radio'.[137] Furthermore, Ofcom does already have some statutory power related to Internet usage. For instance, live streaming subscription services[138] such as Amazon Prime Video is required, in the United Kingdom, to have an Ofcom license alongside complying with the Broadcasting Code.[139] For the Government, Ofcom has the expertise needed to regulate social media companies, whilst also providing a cost-effective mechanism for social media governance.

Though Ofcom would provide a quick, easy and cheap solution to social media regulation, it is important to note that Ofcom already regulates several forms of communications. By allowing Ofcom to also oversee the regulation of social media companies, this could create a monopoly of power which limits the checks and balances in place to ensure freedom of expression is not restricted. To ensure transparency and rigidity a new regulatory body should be created in the form of a Digital Authority, which is overseen by an e-Safety Commissioner[140] using a co-regulatory approach.[141]

Regulatory Body: Digital Authority and e-Safety Commissioner

The proposed Digital Authority in this thesis would oversee the day-to-day regulation of social media companies across the United Kingdom and will be

[137] HM Government n.2, [5.16]
[138] Live steaming subscription service is the process whereby a programme is streamed live and recorded at the same time.
[139] HM Government n.2, [5.28]
[140] The role of the e-Safety Commissioner will be discussed in detail in later parts of this chapter.
[141] Co-regulation, 'is where a regulatory body delegates responsibility to enforce rules to an industry body.' See, Communications Committee n.97, 15. Co-regulation already exists in the United Kingdom for instance, under the Communications Act Ofcom have a statutory duty to regulate broadcasting advertisements, but this has since been delegated to the Advertising Standards Agency.

headed by an e-Safety Commissioner. The Digital Authority would have a number of obligations including, overseeing the implementation of the universal code of conduct, investigating complaints from online users concerning decisions made by social media companies, liaising with the CPS in cases which can be considered as breaching legal provisions, and issue fines to social media companies who fail to adhere to the universal code of conduct.

The proposed Digital Authority would have a similar function to the regulatory body suggested by the Government in their White Paper. Though, instead of the power resting with Ofcom a new independent body will be created. Whereas for the Government '[a] new body would … be more costly to set up and take longer to become operational and risks further complicating the regulatory landscape',[142] it is proposed in this thesis that a new body needs to be created to ensure Ofcom does not become a monopoly of power. Though this will incur a cost and will take time to implement, the Government needs to ensure adequate regulation of social media companies rather than implementing a quick and money-saving approach which may become flawed in the future.[143]

As previously mentioned, the proposed Digital Authority would be headed by an e-Safety Commissioner, endorsing a similar approach to social media

[142] HM Government n.2, [5.15]
[143] For instance, flaws have been exposed with how the United Kingdom currently regulates the press. See, Department for Digital, Culture, Media & Sport and Leveson Inquiry, 'Leveson Inquiry - Report into the culture, practices and ethics of the press' (*Gov.uk*, 29 November 2012) <https://www.gov.uk/government/publications/leveson-inquiry-report-into-the-culture-practices-and-ethics-of-the-press> accessed 23 April 2019

regulation currently being utilised in Australia. As illustrated in Appendix C and D the e-Safety Commissioner, alongside the Digital Authority would be responsible for the creation and implementation of a universal code of conduct.[144] Here, the e-Safety Commissioner and the Digital Authority would work alongside stakeholders such as Facebook, Twitter and not-for-profit organisations to create a universal code of conduct similar to the one proposed in Appendix B.

To ensure adequate checks and balances are in place the e-Safety Commissioner will be responsible for decisions made by the Digital Authority. To protect freedom of expression, a clear and transparent complaints procedure will be implemented for social media companies who wish to challenge a decision made by the Digital Authority. Initial complaints will be made to the e-Safety Commissioner who will ensure that all concerns are reviewed adequately and transparently. All decisions made by the e-Safety Commissioner following a complaint can be referred to the Administrative Court under the principles of Judicial Review. To add further protection, to ensure democracy and free speech is maintained, each year the e-Safety Commissioner will be required to report back to Parliament, as discussed further in Appendix D.

The funds generated by both the voluntary social media levy, and any fines issued to social media companies, will be used to aid educational schemes across the United Kingdom, and help with the costs of continued research

[144] An example of which can be found in Appendix A.

into social media behaviours, to ensure that freedom of speech is not being restricted and all regulatory bodies are working together to help tackle the growing issue of online abuse. An approach that tackles both regulation and education ensures that society keeps pace with the changing nature of technology.

Chapter Overview

The recommendations above may seem complex, but as illustrated throughout this thesis so is online abuse. A multidimensional approach is needed to help tackle the growing issue of inappropriate behaviours online. As has been illustrated at various points in this thesis the current system of self-regulation is not working.

This thesis recommends the following changes:

The Law

- Create clear and precise legal rules regulating online conduct and abuse in the form of a coherent Bill, whilst also ensuring provisions are in place to protect freedom of expression;
- Produce a clear and precise legal rule regulating the encouragement of another to either commit a further criminal offence or incite others to target another online;
- Create a clear and precise legal rule regulating online hate speech. Here, what constitutes hate speech should be expanded;
- Specifically criminalise cyber harassment and cyberstalking ensuring a clear and precise definition is created;

- Adapt section 33 of the Criminal Justice and Courts Act 2015 to expand the *mens rea* of the offence to include recklessness;
- Expand the definition of 'sexual imagery' in relation to revenge pornography;
- Prohibit revenge pornography in the form of fake images or videos;
- Ensure anonymity is given to victims of revenge pornography;
- Include a clear and precise definition of false communications with the aid of case law examples; and
- Define grossly offensive and menacing material with the aid of case law examples and the CPS guidelines on social media prosecutions.

Social Media Prosecuting Guidelines

- Ensure the social media prosecuting guidelines are updated to include examples to illustrate when a comment or conduct breaches legal provisions, taking into consideration both privacy and freedom of expression;
- The inclusion of the Computer Misuse Act 1990 in the CPS social media prosecuting guidelines; and
- Give better protection for victims of online abuse in particular ensuring someone's right to privacy is maintained in a digital age.

Training and Education

- Better training for police forces as to what constitutes harassment and stalking, especially those conducted online;

- Ensure better education is given to the police and social media users concerning the psychological effects of online abuse;
- Digital training for police officers to ensure they fully understand the effects of online abuse on those who are subjected to it; and
- Create better educational schemes for children, parents and law enforcement in relation to digital literacy skills.

Social Media Companies

- Create a universal code of conduct aimed at all social media companies to ensure they are protecting individuals from online abuse. The universal code of conduct needs to be created in a clear and precise manner;
- Guarantee social media companies are transparent with their users;
- Updated training on a regular basis for moderators;
- Ensure social media companies aid law enforcement; and
- Where social media companies fail to comply with the universal code of conduct create a punishment process in the form of a fine, governed by the e-Safety Commissioner and the Digital Authority.

Governance

- Create a harmonised approach between legislation and non-legislative provisions governing online abuse;
- The creation of a Digital Authority headed by an e-Safety Commissioner overseeing the regulation of social media companies;

- Create a transparent reviewing system of all legal provisions implemented to govern social media abuse to ensure democracy is maintained, and freedom of speech is not curtailed; and
- Any legal provisions that are created ensure that the advancements in new technology or new social media companies are not restricted.

Conclusion

> 'In our view, good regulation is not only about restricting certain types of conduct; rather, it makes the digital world work better for everyone and engenders a more respectful and trustworthy culture.'[1]

Research findings and limitations

This thesis set out to examine the extent to which the current criminal law framework, social media companies and society can better govern abusive conduct aided by social media. It has found that the current use of adapting legislative provisions, some of which were never intended to cover the internet, let alone social media, leaves two significant issues: the law is failing to adequately protect those subjected to online abuse and the law in some cases is being used arbitrarily. In addition, it is clear from previous discussions that social media gatekeepers need to do more to protect their users from abusive behaviour. However, to better protect victims of online abuse and ensure adequate regulation, changes are needed throughout society, such as educational schemes, before it can be said that we are tackling the growing issue of online abuse.

The recommendations put forward in this thesis have therefore been influenced from examining the current criminal law framework from the perspective of legality, alongside investigating how the likes of Facebook and Twitter have attempted to tackle abusive behaviour on their sites. To enrich the recommendations, chapter eight evaluated how other countries and

[1] Communications Committee, *Regulating in a digital world* (HL 2017-19, 299) [19]

institutions have attempted to govern abusive behaviour online. However, like all studies, there are some limitations:

- It can be suggested that some arguments put forward in this thesis attempt to justify the actions of the perpetrator by proposing that they have been prosecuted or convicted under the wrong Act of Parliament. However, this is not the case but by taking a non-consequentialist approach, the researcher is interested in the process undertaken in determining which Act of Parliament should be applied in a given situation. At no point does the researcher wish to justify the actions of abusing another online.
- Flaws may exist within the proposed Social Media Bill. However, the Social Media Bill put forward in Appendix A is considered the foundational point in attempting to create legal provisions which comply with the principle of legality. At no point does the researcher believe that the Bill should receive royal assent in its current format, it is simply a draft provision which will be further strengthened by discussions with other interested parties, such as non-government organisations.
- It is accepted that other theoretical perspectives and methods could have been utilised to strengthen the research. However, as outlined in chapter two, legality can be considered the foundation of the criminal justice system on which all legal provisions should be built upon. Consequently, the principle of legality was used as the theoretical perspective underpinning this thesis as without legality, it leaves open

the possibility that the law can be used arbitrarily, in which serious misunderstandings can occur throughout the criminal justice system.

Chapter Summary and Final Remarks

The advancement of changing technology has altered many aspects of society, from how we obtain our news to changing how individuals communicate with others. As discussed in chapter one social media has been prevalent in this change. Though this thesis has illustrated the darker side of social media, it can and has, been a force for good. In recent years society has seen campaigns to create changes within the UK's criminal justice system,[2] campaigns to highlight the continued abuse of women within society,[3] and campaigns to end the stigma surrounding domestic violence,[4] all of which have been aided by social media. Social media allows individuals to connect instantly across the globe and keep updated with world events. However, it does have a darker side in which misogyny, harassment and revenge pornography, to name but a few can flourish.

Chapter one exposed the growing issues of online abuse. Though there is no agreed definition of online abuse or indeed abuse, it has come to be accepted that certain behaviours can constitute abuse online. For instance,

[2] For example, campaigns surrounding the criminalisation of upskirting. See, Katie O'Malley, 'What Is Upskirting And When Did It Become A Criminal Offence?' *The Independent* (London, 12 April 2019) <https://www.independent.co.uk/life-style/women/upskirting-illegal-definition-crime-uk-sexual-harassment-a8864636.html> accessed 24 April 2019

[3] Bri Lee, 'Sharing our stories is the strength at the heart of #MeToo. We must repeal gag laws' *The Guardian* (London, 19 November 2018) <https://www.theguardian.com/commentisfree/2018/nov/19/sharing-our-stories-is-the-strength-at-the-heart-of-metoo-we-must-repeal-gag-laws> accessed 27 November 2018

[4] Jessamy Gleeson, '"(Not) working 9–5": the consequences of contemporary Australian-based online feminist campaigns as digital labour' (2016) 16(1) Media International Australia 77 <http://journals.sagepub.com/doi/pdf/10.1177/1329878X16664999>

concerns have been repeatedly raised about cyberbullying, particularly its effects on the younger generation:

> 'We know that bullying is not a new phenomenon, but the digital landscape has fundamentally changed the way that young people are experiencing it. It is increasingly the case that children are being bullied online through social media platforms and the complexity of these social networks means bullying can take on different forms on different platforms.'[5]

Cyberbullying can have a detrimental effect on a person's wellbeing. For instance, a survey conducted by Ditch the Label in 2017 found that of those who had suffered cyberbullying, 41% had developed anxiety, 37% developed depression, 26% experienced suicidal thoughts, with 25% of participants identifying that they had self-harmed because of cyberbullying.[6] However, online abuse does not just affect the younger generation, anyone can become a victim of abuse online.

In 2013 following a public campaign to get the author Jane Austin printed on banknotes in the United Kingdom, Caroline Criado-Perez, was subjected to a crusade of misogynistic abuse online.[7] Comments included, 'rape her nice arse', 'I will fuck you at 9pm … shall we meet near your house', and 'If your friends survived rape, they weren't raped properly [*sic*]'. At its height, Ms

---

[5] The Children's Society, 'Safety Net: Cyberbullying's impact on young people's mental health Inquiry report' (*The Children's Society*, 2018) <https://www.childrenssociety.org.uk/sites/default/files/social-media-cyberbullying-inquiry-full-report_0.pdf> accessed 24 April 2019

[6] Ditch the Label, 'The Annual Bullying Survey 2017' (*Ditch the Label*, 2017) <https://www.ditchthelabel.org/wp-content/ uploads/2017/07/The-Annual-Bullying-Survey-2017-2.pdf> accessed 24 April 2019

[7] Alexandra Topping, 'Jane Austen Twitter row: two plead guilty to abusive tweets' *The Guardian* (London, 7 January 2014) <https://www.theguardian.com/society/2014/jan/07/jane-austen-banknote-abusive-tweets-criado-perez> accessed 10 October 2016

Criado-Perez was receiving 50 highly abusive messages per hour.[8] Similarly, Jess Phillips an MP from the Birmingham area has publicly spoken about receiving more than 600 threats of rape in one night alone *via* Twitter.[9]

Whereas chapter one provided a contextualisation as to why research into social media abuse was needed, chapter two outlined the theoretical position of this thesis, legality. To justify using the perspective of legality to review the criminal law framework, chapter two outlined other theoretical perspectives which could have been utilised, including deterrence theory, rational choice theory, feminism, digital feminism and victimology. However, it was decided that legality was the appropriate theoretical position to use for the research questions posed as it allowed the researcher to criticise the law from both the perspective of the victim and the perpetrator; illustrating the fundamental flaws in applying outdated legislation to unlawful behaviour aided by social media.

To fully understand the continuing issues in governing online abuse, chapter three examined in detail the mechanisms Facebook and Twitter have implemented on to their sites to help reduce and control inappropriate behaviours online. Yet despite both companies continuingly investing in Artificial Intelligence Technology and moderators, Twitter and Facebook are failing to keep pace with unlawful and harmful content which is flourishing

[8] The BBC, 'Caroline Criado-Perez Twitter abuse case leads to arrest' *The BBC* (London, 29 July 2013) <https://www.bbc.co.uk/news/uk-23485610> accessed 8 February 2019
[9] Sally Hayden, 'Labour's Jess Phillips received "600 rape and death threats in a single day"' *The Independent* (London, 27 August 2017) <http://www.independent.co.uk/news/uk/home-news/labour-mp-jess-phillips-rape-death-threats-one-day-social-media-attacks-training-a7915406.html> accessed 25 October 2017

across their sites, resulting in other agencies and law enforcement having to intervene; justifying as to why social media companies need to do more in order to reduce unlawful and abusive behaviour on their sites, whilst also emphasising the need for strong legal provisions.

In England and Wales, there is no specific Act of Parliament governing conduct carried out online. Instead, Acts have been adapted to fit a digital age. In chapter four the Serious Crime Act 2007, the Public Order Act 1986 and the Protection from Harassment Act 1997 were examined. These three Acts can be defined as non-technology-based laws yet have since been used to control unlawful behaviours online. The application of these Acts in a digital context has given rise to several issues. For example, the Serious Crime Act was never intended to cover social media abuse, instead its purpose was to target the most serious and organised crime across the United Kingdom, for instance human trafficking, drug offences and money laundering. Despite this, in 2011 part three of the Serious Crime Act was used to convict two individuals for inciting others *via* Facebook to participate in disorderly behaviour.

In August 2011 following the shooting of Mark Duggan by armed police, riots started to emerge across the country.[10] During the height of the riots two individuals, Jordan Blackshaw[11] and Perry Sutcliffe-Keenan[12] took to

[10] Vikram Dodd & Caroline Davies, 'London riots escalate as police battle for control' *The Guardian* (London, 9 August 2011) <https://www.theguardian.com/uk/2011/aug/08/london-riots-escalate-police-battle> accessed 3 November 2011
[11] *R v Jordan Blackshaw* Chester Crown Court 16 August 2011 (unreported)
[12] *R v Perry Sutcliffe-Keenan* Chester Crown Court 16 August 2011 (unreported)

Facebook to create public event pages to incite others to become involved in disorderly behaviour. Despite the riots they attempted to organise not taking place both individuals were prosecuted and convicted to 4 years imprisonment under the Serious Crime Act. Similarly, in 2012 the Public Order Act was used to successfully convict Liam Stacey for the sending of racist and obscene messages *via* Twitter, following the collapse of Bolton Wanderers star Fabrice Muamba during a football match.[13]

The use of these two Acts of Parliament, the Serious Crime Act and the Public Order Act, can be considered as a breach of the principle of legality in the criminal law. As outlined above the principle of legality is considered the idea that the law should be accessible and clear to guide citizens.[14] As argued in chapter four the use of the Serious Crime Act and the Public Order Act to prosecute social media offences can be considered as outside Parliament's original intentions and therefore, cannot be considered as a guiding mechanism for citizens within England and Wales.

Chapter four also exposed growing concerns in the use of the Protection from Harassment Act in a social media context. In the legal system of England and Wales, the terms harassment and stalking have no definitive definition, meaning they are often misunderstood by the police and the Crown Prosecution Service (CPS).[15] This has resulted in devastating

[13] *R V Liam Stacey* Swansea Crown Court On Appeal From The Magistrates' Court A20120033
[14] Joseph Raz, *The Authority of Law* (Oxford University Press 1979) 218
[15] Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate, 'Living in fear – the police and CPS response to harassment and stalking' (*justiceinspectorates.gov*,

consequences for victims of this form of abuse, especially when the behaviour is conducted or aided by modern technology.[16] The lack of a clear and accessible meaning to these terms, in line with the principle of legality, means those who are subjected to cyber harassment or cyberstalking are often let down by the criminal justice system.

Chapter five discussed in detail the use of the Computer Misuse Act 1990 and section 33 of the Criminal Justice and Courts Act 2015. Both these provisions were created and implemented with digital technology in mind, though the Computer Misuse Act may not have necessarily been implemented to govern social media. As outlined in chapter five both these provisions conform to the principle of legality. Though section 33 of the Criminal Justice and Courts Act, which criminalises revenge pornography, is not without fault. In law a narrow definition is given to the offence of distributing an explicit image of another. For instance, a person can only be convicted of revenge pornography if they send a sexually explicit image of another to cause distress. Consequently, images sent for say financial gain are outside the realms of the Act. Issues have also arisen with the lack of anonymity given to those who are subjected to revenge porn.

Despite several Acts and provisions currently being utilised in a social media context as discussed in chapter six, section 127 of the Communications Act 2003 and the Malicious Communications Act 1988 have become prevalent in

July 2017) <http://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/living-in-fear-the-police-and-cps-response-to-harassment-and-stalking.pdf> accessed 29 November 2017

[16] Laura Bliss, 'The Protection from Harassment Act 1997: Failures by the Criminal Justice System in a Social Media Age' 83(3) Journal of Criminal Law 217

governing conduct carried out online. Both provisions can be considered as similar, which has resulted in them becoming interchangeable within the criminal justice system.[17] Between the two provisions, it is an offence to send an indecent, obscene, menacing, false, threatening or a grossly offensive communication; though issues have arisen regarding the meaning of these terms, particularly the meaning of grossly offensive or menacing messages.

As outlined in chapter six when it comes to grossly offensive messages, there is a boundary between offensive commentary, which is protected under Article 10 of the European Convention on Human Rights and Fundamental Freedoms, and grossly offensive commentary which is not. However, the issue remains as to where the boundary lies between the two, as clearly illustrated in *R v Woods*[18] and the matter of Daniel Thomas.[19]

Thomas who at the time was a Port Talbot footballer, took to Twitter to post the following comment: 'if there is any consolation for finishing fourth at least [*sic*] daley and waterfield [*sic*] can go bum each other #teamHIV'.[20] Despite the homophobic and offensive nature of the tweet, a decision was made by the CPS not to prosecute.[21] Whereas in *Woods*, the defendant was convicted under section 127(1) of the Communications Act for the sending of grossly offensive material, following comments posted on Facebook concerning a

[17] Laura Scaife, *Handbook of Social Media and the Law* (Routledge 2015) 166
[18] *R v Matthew Woods*, Chorley Magistrates Court, 8 October 2012 (unreported)
[19] The Crown Prosecution News Brief, 'DPP Statement on Tom Daley Case and Social Media Prosecutions' (*CPS.gov,* 2012) <http://blog.cps.gov.uk/2012/09/dpp-statement-on-tom-daley-case-and-socialmedia-prosecutions.html> accessed 29 April 2018
[20] *Ibid.,*
[21] *Ibid.,*

missing schoolchild in Wales. Comments included, 'I woke up this morning in the back of a transit van with two beautiful little girls, I found April in a hopeless place.' 'Could have just started the greatest Facebook argument EVER [*sic*]. April fools, who wants Maddie? I love April Jones.'[22] In essence:

> '[i]t is perhaps easy to see why the comments made by Woods were grossly offensive and so worthy of prosecution. It is less obvious why those made by Thomas were not. Or, to put the matter more pertinently, if the two cases of Woods and Thomas are on either side of a line between comments which are merely offensive and those which are grossly so, the question arises as to where that line lies.'[23]

Similar issues have arisen concerning menacing communications as highlighted in the case of *R v Chambers*,[24] discussed in detail in chapter six.

Chapter seven examined two significant rights when it comes to governing conduct carried out online: freedom of expression versus a person's right to privacy, which need to be balanced against each other. Freedom of expression is an important aspect of any democratic society and is given significant protection by the European Court of Human Rights,[25] but as discussed in chapter seven it is not an absolute right. Consequently, a person's right to free speech can be restricted when three criterions are met: the restriction is governed by law, the restriction achieves one of the legitimate aims contained in the second paragraph of the right, and the restriction is necessary in a democratic society. Likewise, privacy is also a

---

[22] Steven Morris & Dan Sabbagh, 'April Jones: Matthew Woods jailed over explicit Facebook comments' *The Guardian* (London, 8 October 2012) <https://www.theguardian.com/uk/2012/oct/08/april-jones-matthew-woods-jailed> accessed 29 April 2018

[23] Laura Bliss, 'The crown prosecution guidelines and grossly offensive comments: an analysis' (2017) 9(2) Journal of Media Law 173, 177

[24] *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin), [2013] 1 WLR 183

[25] *Handyside v United Kingdom* (1976)1 EHRR 737

qualified right. However, privacy as exposed in varies points of this thesis is more than the protection of a person's private life, it encompasses a right not to have ones physical and physiological integrity breached.

As highlighted in chapter seven a person's right to privacy needs to be taken into consideration when it comes to restricting online behaviours, alongside that of freedom of expression. Currently, the criminal justice system tilts in the direction of freedom of expression. This thesis has argued that privacy needs to be taken into consideration first before that of freedom of expression. Consequently, the proposed changes put forward in this thesis more adequately protects individuals from online abuse, and in turn protects their right to privacy.

To conclude this thesis several recommendations have been put forward, aided by examining how other institutions and countries are currently tackling unlawful behaviours. The rationale on focussing on the European Union, Australia, Germany and India relate to the different approaches each have taken in attempting to combat the same issue, online abuse. Chapter eight therefore exposed that there is not just one universal approach to Internet governance. The European Union and Australia have both implemented legislative and non-legislative approaches to deal with inappropriate behaviours online. Whereas Germany and India, have endorsed a legislative approach to tackling online abuse aimed at either the social media provider or the online user. The discussions in chapter eight underpin many of the recommendations put forward in chapter nine.

Chapter nine argued that a multidimensional approach to social media regulation was needed. The Social Media Bill as located in Appendix A has attempted to overcome issues highlighted throughout various points of this thesis. The Bill includes a clear and accessible definition of the term's cyber harassment and cyberstalking, specifically criminalises dogpiling and provides a definition of the term's grossly offensive and menacing communications. In addition, the Bill creates a wider definition of revenge pornography to reflect the detrimental effects this form of abuse can have on another. However, both legislative and non-legislative approaches are needed to keep pace with changing technology. Therefore, it has been proposed that a Digital Authority should be created to oversee the regulation of social media companies, headed by an e-Safety Commissioner. In turn, a universal code of conduct needs to be created alongside universal digital education.

Social media is of paramount importance within society, but the darker side of this relatively new form of communication can have detrimental effects on both a person's mental and physical wellbeing. This thesis set out to investigate how the current criminal law framework deals with online abuse. It is clear from previous chapters that the current approach to shaping and adapting legal provisions to fit a social media context is failing to protect those who are abused online. We must therefore act now to help tackle the growing issue of online abuse.

Future Research

- Engaging with non-government organisations and other interested parties such as victims and gatekeepers to strengthen the recommendations put forward in this thesis;
- Interviewing actors in the criminal justice system and victims of online abuse to get their opinions on the current regulation of social media; and
- Further examination of how other countries and institutions are attempting to tackle online abuse.

Bibliography

Books

Abbott P, Wallace C & Tyler M, *An Introduction to Sociology: Feminist Perspectives* (3rd ed, Routledge 2005)

Allen M J, *Criminal Law* (14th edn, Oxford 2017)

Ashworth A & Horder J, *Principles of Criminal Law* (7th edn, Oxford University Press 2013)

Babbie E, *The Basics of Social Research* (Cengage Learning 2007)

Baldwin T, *Ctrl Alt Delete: How Politics and the Media Crashed Our Democracy* (Oxford University Press 2018)

Bandura A, *Principles of Behavior Modification* (Holt, Rinehart and Winston 1969)

Barnett H:

Constitutional & Administrative Law (12th edn, Routledge 2017)

Constitutional & Administrative Law (5th edn, Cavendish Publishing 2004)

Beale A, *Essential Constitutional Law* (2nd edn, Cavendish Publishing Limited 1997)

Bell D J, Loader B D, Pleace N & Schuler D, *Cyberculture: The Key Concepts* (Routledge 2004)

Bernal P, *The Internet, Warts and All: Free Speech, Privacy and Truth* (Cambridge University Press 2018)

Bocij P, *Cyberstalking: Harassment in the Internet Age and how to Protect Your Family* (Praeger Publishers 2004)

Bowling B & Phillips C, 'Racist Victimisation in England and Wales' in Hawkins D F (ed), *Violent Crime: Assessing Race and Ethnic Differences* (Cambridge University Press 2003)

Brenner S W, *Cybercrime: Criminal Threats from Cyberspace* (Greenwood Publishing Group 2010)

Cockburn C, *Brothers: Male Dominance and Technological Change* (Pluto Press 1983)

Criado-perez C, *Invisible Women: Exposing Data Bias in a World Designed for Men* (2019 Chatto & Windus)

Davis M, Croall H & Tyrer J, *Criminal Justice* (4th edn, Pearson Education 2010)

de Beauvoir S*, The Second Sex* (Vintage 1949)

Deo Gaur K, *Textbook on the Indian Penal Code* (Universal Law Publishing 2009)

Desborough J, *Inside Gamergate: A Social History of the Gamer Revolt* (Lulu.com 2017)

Dickson R, Cherry M C and Boland A, 'Carrying Out a Systematic Review as a Master's Thesis' in Boland A, Cherry M C & Dickson R (eds) *Doing a Systematic Review: A student's Guide* (2nd edn, Sage 2014)

Disch L & Hawkesworth M (eds) *The Oxford Handbook of Feminist Theory* (Oxford University Press 2016)

Douget A & Mauthner N S, 'Feminist Methodologies and Epistemology' in Bryant C D & Peck D L (eds), *Handbook of 21st Century Sociology* (Sage 2006)

Elliot M & Thomas R, *Public Law* (3rd edn, Oxford University Press 2017)

Fafinski S, *Computer Misuse* (Routledge 2009)

Fattah E A, 'Victims and Victimology: The Facts and the Rhetoric' in Fattah E A (ed), *Towards a Critical Victimology* (Palgrave 1992)

Fletcher G P, *Basic Concepts of Criminal Law* (Oxford University Press 1998)

Fontaine R G, *The Mind of the Criminal: The Role of Developmental Social Cognition in Criminal Defense Law* (Cambridge University Press 2012)

Fuchs C, *Social Media a Critical Introduction* (Sage Publications 2014)

Fuller L L, *The morality of law* (Yale University Press 1964)

Fry M, *Arms of the law* (Howard League for Penal Reform by Gollancz 1951)

Goodey J, *Victims and Victimology: Research, Policy and Practice* (Pearson Education Ltd 2005)

Guilfoyle D, *International Criminal Law* (Oxford University Press 2016)

Hall N, *Hate Crime* (2nd edn, Routledge 2013)

Heberle R, 'The Personal is Political' in Disch L & Hawkesworth M (eds) *The Oxford Handbook of Feminist Theory* (Oxford University Press 2016)

Hentig H V, *The Criminal and his Victim: studies in the Sociobiology of Crime* (Yale University Press 1948)

Holt T J, Bossler A M & Seigfried-Spellar K C, *Cybercrime and Digital Forensics: An Introduction* (2nd edn, Routledge 2017)

Horsey K & Rackley E, *Tort Law* (4th edn, Oxford University Press 2015)

Jackson J C, *Web Technologies: A Computer Science Perspective* (Pearson Education 2007)

Karmen A, *Crime Victims: An Introduction to Victimology* (Cengage Learning 1990)

Kearon T & Godfrey B S, 'Setting the scene: a question of history' in Walklate S (ed), *Handbook of Victims and Victimology* (Routledge 2011)

Lipschultz J H, *Social Media Communication: Concepts, Practices, Data, Law and Ethics* (2nd edn, Routledge 2018)

Lowe F (ed), 'The August 2011 Riots- Them and Us' in *Thinking Space: Promoting about Race, Culture, and Diversity in Psychotherapy and Beyond* (Karnac Books 2014)

Luban D, 'Fairness to rightness: Jurisdiction, Legality, and the Legitimacy of International Criminal Law' in Besson S & Tasioulas J (eds), *The Philosophy of International Law* (Oxford University Press 2010)

Martin J & Storey T, *Unlocking Criminal Law* (4th edn, Routledge 2013)

Masterman R, *The Separation of Powers in the Contemporary Constitution: Judicial Competence and Independence in the United Kingdom* (Cambridge University Press 2010)

Mawby R & Walklate S, *Critical Victimology* (Sage 1994)

*Mendelsohn B, '*Une *nouvelle* branche de la science bio-psycho-sociale: la *victimologie' (1956) Revue internationale de criminologie et de police technique* found in Mawby R & Walklate S, *Critical Victimology* (Sage 1994)

Mendes K, Ringrose J & Keller J, *Digital Feminist Activism: Girls and Women Fight Back Against Rape Culture* (Oxford University Press 2019)

Millet K, *Sexual Politics (*Avon Books 1971)

Moore R, *Cybercrime: Investigating High-Technology Computer Crime* (2nd edn, Routledge 2011)

Murray A D, 'Mapping the rule of law for the internet' in Mangan D & Gillies L E (eds), *The Legal Challenges of Social Media* (Edward Elgar Publishing 2017)

Murray A, *Information Technology Law: The Law and Society* (3rd edn, Oxford University Press 2016)

Powell A & Henry N, *Sexual Violence in a Digital Age* (Springer 2017)

Powell A, Stratton G & Cameron R, *Digital Criminology: Crime and Justice in Digital Society* (Routledge 2018)

Raz J, *The Authority of Law* (Oxford University Press 1979)

Reed C, *Internet Law: Text and Materials* (Cambridge University Press 2004)

Reimann P, 'Communities in practice' in Adelsberger H M *et al* (eds), *Handbook on Information Technologies for Education and Training* (2nd edn, Springer 2008)

Rogers K M, *The Internet and the Law* (Macmillan International Higher Education 2011)

Scaife L, *Handbook of Social Media and the Law* (Routledge 2015)

Shelly G B & Campbell J, *Discovering the Internet: Brief* (Cengage Learning 2011)

Shin K Y, 'Goverance' in Disch L & Hawkesworth M (eds) *The Oxford Handbook of Feminist Theory* (Oxford University Press 2016)

Shirky C, *Here comes everyone* (Penguin 2008)

Smartt U, *Media & Entertainment Law* (Taylor & Francis 2017)

Sparks R, 'Prison, Punishment and Penality' in McLaughlin E & Muncie J, *Controlling Crime* (2nd end, The Open University 2001)

Veletsianos G 'The Defining Characteristics of Emerging Technologies and Emerging Practises in Digital Education' in Veletsianos G (ed), *Emergence and Innovation in Digital Learning: Foundations and Applications* (Athabasca University Press 2016)

Weimann G, 'Why do terrorists migrate to social media?' in Aly A, Macdonald S, Jarvis L & Chen T (eds), *Violent Extremism Online: New Perspectives on Terrorism and the Internet* (Routledge 2016)

Wellman B & Haythornthwaite C (eds), *The Internet in Everyday Life* (John Wiley & Sons 2008)

William R, 'Fighting "Fake News" in the Age of Digital Disorientation: Towards "Real News" Critical Media Literacy Education, and Independent Journalism for 21st Century Citizens' in Goering C Z & Thomas P L (eds), *Critical Media Literacy and Fake News in Post-Truth America* (BRILL 2018)

Williams K S, *Textbook on Criminology* (7th edn, Oxford University Press 2012)

Wilson S, Rutherford H, Storey T & Wortley N, *English Legal System* (2nd edn, Oxford University Press 2016)

Woods L, 'Social Media: it is not just about Article 10' in Mangan D & Gillies L E (eds), *The Legal Challenges of Social Media* (Edward Elgar Publishing 2017)

Journal Articles

Agate J & Ledward J, 'Social media: how the net is closing in on cyber bullies' (2013) 24(8) Entertainment Law Review 263

Akhar Z, 'Malicious communications, media platforms and legal sanctions' (2014) 20(6) Computer and Telecommunications Law Review 179

Allen M, 'What was Web 2.0? Versions as the dominant mode of internet history' (2012) 15(2) New Media & Society 260

Banks J, 'Regulating hate speech online' (2010) 24(3) International Review of Law Computers & Technology 233

Barak A, 'Sexual Harassment on the Internet' (2005) 23(1) Social Science Computer Review 77

Bates B, 'Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors' (2017) 12(1) Feminist Criminology 22

Becker G, 'Crime and Punishment: An Economic Approach' (1968) 76(2) Journal of Political Economy 169

Bernstein A, 'Abuse and Harassment Diminish Free Speech' (2014) 35 Pace Law Review 1

Birkbeck S, ‘Can the use of social media be regulated?’ (2013) 19(3) Computer and Telecommunications Law Review 83

Bliss L:

‘The Protection from Harassment Act 1997: Failures by the Criminal Justice System in a Social Media Age’ (2019) 83(3) Journal of Criminal Law 217

‘Social Media: “A Theme Park just for Fools”’ (2018) 82(4) The Journal of Criminal Law 301 (note)

‘The crown prosecution guidelines and grossly offensive comments: an analysis’ (2017) 9(2) Journal of Media Law 173

Broadbent G, ‘Malicious Communications Act 1988: human rights’ (2007) 71(4) Journal of Criminal Law 288

Chambers A D, ‘Computer fraud and abuse’ (1977) 21(3) The Computer Journal 194

Chesney-Lind M, ‘Patriarchy, Crime, and Justice’ (2006) 1(1) Feminist Criminology 6

Child J J, ‘Exploring the mens rea requirements of the Serious Crime Act 2007 assisting and encouraging offences’ (2012) 76(3) Journal of Criminal Law 220

Christie A L, ‘Should the law of theft extend to information?’ (2005) 69(4) Journal of Criminal Law 349

Citron D K, ‘Cyber Civil Rights’ (2008) 89 Boston Law Review 61

CM A, ‘E-Commerce Law in Developing Countries: An Indian Perspective’ (2002) 11(3) Information & Communications Technology Law 269

Cook C, Schaafsma J & Antheeunis M, ‘Under the bridge: an in-depth examination of online trolling in a gaming context’ (2017) 20(9) New Media & Society 3323

Craig P, ‘Formal and substantive conceptions of the rule of law: an analytical’ (1997) Public Law 467

Dempsey S E, ‘The Increasing Technology Divide: Persistent portrayals of maverick masculinity in US marketing’ (2009) 9(1) Feminist Media Studies 37

Driscoll J, ‘Protest and Public Order: The Public Order Act 1986’ (1987) Sep Journal of Social Welfare Law 280

Edwards L, ‘Section 127 of the Communications Act 2003: Threat or Menace?’ (2012) 23(4) Computers & Law 22

Foster S, ‘Freedom of expression: is there a human right to make a joke?’ (2012) 17(2) Coventry Law Journal 97

Geach N & Haralambous N, ‘Regulating harassment: is the law fit for the social networking age?’ (2009) 73(3) Journal of Criminal Law 241

Geerken M & Grove W, ‘Deterrence: Some Theoretical Considerations’ (1975) 9(3) Law and Society 497

Geiger S, ‘What’s So Feminist about Women’s Oral History?’ (1990) 2(1) Journal of Women’s History 169

Gelman L, ‘Privacy, Free Speech, and “Blurry Edged” Social Networks’ (2009) 50(5) Boston Collage Law Review 1315

Gibbon T, ‘Case Comment: Grossly offensive communications’ (2006) 11(4) Communications Law 136 (note)

Gillespie A A:

‘“Trust me, it's only for me”: “revenge porn” and the criminal law’ (2015) 11 Criminal Law Review 866

‘Twitter, jokes and the law’ (2012) 76(5) Journal of Criminal Law 364 (note)

‘Offensive communications and the law’ (2006) (17)8 Entertainment Law Review 236

Gowland J, ‘Protection from Harassment Act 1997: the "new" stalking offences’ (2013) 77(5) Journal of Criminal Law 387

Griffiths R, ‘Social media and the criminal law’ (2013) 24(2) Entertainment Law Review 57

Hamilton P & Spongberg M, ‘Twenty Years On: feminist histories and digital media’ (2016) 26(5) Women’s History Review 671

Hammond G, ‘Theft of Information’ (1988) 104(Oct) Law Quarterly Review 527

Haralambous N & Geach N, ‘Online Harassment and Public *Dis*-order’ (2010) 174 Criminal Law and Justice Weekly 409

Jackson S, ‘Young Feminists, Feminism and Digital Media’ 2018 28(1) Feminism & Psychology 32

Jane E A, ‘Online Misogyny and Feminist Digilantism’ (2016) 30(3) Journal of Media and Cultural Studies 284

John A *et al*, ‘Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review’ (2018) 20 (4) Journal of Medical Internet Research 129

Johnson D & Post D, ‘Law and Borders: The Rise of Law in Cyberspace’ (1996) 48 Stanford Law Review 1367

Jungherr A *et al*, ‘Digital Trace Data in the Study of Public Opinion: An Indicator of Attention Toward Politics Rather Than Political Support’ (2017) 35(3) Social Science Computer Review 336

Kamal M & Newman W J, ‘Revenge Pornography: Mental Health Implications and Related Legislation’ (2016) 44(3) American Academy of Psychiatry and the Law 359

Kirchengast T, ‘The Limits of the Criminal Law and Justice: “Revenge Porn” Criminalisation, hybrid responses, and the ideal victim’ (2016) 2 UniSA Student Law Review 96

Ledward J & Agate J, ‘“Revenge porn” and s.33: the story so far’ 28(2) Entertainment Law Review 40

Lewis R, Rowe M & Wiper C, ‘Online Abuse of Feminists as an Emerging form of Violence Against Women and Girls’ (2017) 57 British Journal of Criminal Law 1462

Li Q, ‘Cyberbullying in High Schools: A Study of Students’ Behaviors and Beliefs about This New Phenomenon’ (2010) 19(4) Journal of Aggression, Maltreatment & Trauma 372

Lightowlers C & Quirk H, ‘The 2011 English “Riots”: Prosecutorial Zeal and Judicial Abandon’ (2015) 55(1) British Journal of Criminology 65

Lilienthal G & Ahmad N, ‘Hate crime and social media in the UK’ (2016) 22(7) Computer and Telecommunications Law Review 188

Lord Bingham, ‘The rule of law’ (2007) 66(1) Cambridge Law Journal 67

MacEwan N:

‘The new stalking offences in English law: will they provide effective protection from cyberstalking?’ (2012) 10 Criminal Law Review 767

‘The Computer Misuse Act 1990: lessons from its past and predications for its future’ (2008) 12 Criminal Law Review 955

Margetts H, ‘Why Social Media May Have Won the 2017 General Election’ (2017) 88(3) The Political Quarterly 386

Mitchell B, ‘Sentencing riot-related offending: considering Blackshaw and others’ (2011) 10 Archbold Review 4

Mitchell J, ‘Censorship in cyberspace: closing the net on “revenge porn”’ (2014) 25(8) Entertainment Law Review 283

Morris J, ‘The structure of criminal law and deterrence’ (1986) Aug Criminal Law Review 524

Murphy C C, ‘The principle of legality in criminal law under the European Convention on Human Rights’ (2010) 2 European Human Rights Law Review 192

Nehaluddin A, ‘Hackers’ criminal behaviour and laws related to hacking’ (2009) 15(7) Computer and Telecommunications Law Review 159

Norrie A W, ‘Oblique intention and legal politics’ (1989) Nov Criminal Law Review 793

Paternoster R, ‘How much do we really know about criminal deterrence’ (2010) 100 (3) Journal of Criminal Law and Criminology 765

Pathé M & Mullen P, ‘The impact of stalkers on their victims’ (1997) 170(1) The British Journal of Psychiatry 12

Payne D L, Lonsway K A, & Fitzgerald L F, ‘Rape myth acceptance: Exploration of its structure and its measurement using the Illinois Rape Myth Acceptance Scale’ (1999) 33 Journal of Research in Personality 27

Plater D, ‘“Setting the boundaries of acceptable behaviour?” South Australia’s latest legislative response to revenge pornography’ (2016) 2 UniSA Student Law Review 77

Raz J, ‘The Rule of Law and its Virtue’ (1977) 93 Law Quarterly Review 195

Rizzuto F, ‘Case Comment: Injunctions against intermediate online service providers’ (2012) 18(3) Computer and Telecommunications Law Review 69 (note)

Rowbottom J, ‘To rant, vent and converse: protecting low level digital speech’ (2012) 71(2) Cambridge Law Review 355

Salter M & Bryden C, ‘I can see you: harassment and stalking on the Internet’ (2009) 18(2) Information & Communications Technology Law 99

Sanz-Caballero S, ‘The principle of nulla poena sine lege revisited: the retrospective application of criminal law in the eyes of the European Court of Human Rights’ (2017) 28(3) European Journal of International Law 787

Sarosh Khan, ‘Can the trolls be put back under the bridge?’ (2013) 19(1) Computer and Telecommunications Law Review 9

Scaife L, ‘The DPP and social media: a new approach coming out of the Woods?’ (2013) (18)1 Communications Law 5

Sears A, ‘Protecting Freedom of Expression over the Internet: An International Approach’ (2015) 5(1) Notre Dame Journal of International & Comparative Law 171

Spencer J & Virgo G, ‘Encouraging and assisting crime: legislate in haste, repent at leisure’ (2008) 9 Archbold News 7

Stratton G, Powell A & Cameron R, ‘Crime and Justice in Digital Society: Towards a Digital Criminology?’ (2016) 6(2) International Journal for Crime, Justice and Social Democracy 17

Stroud S R, ‘The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn’ (2014) 29(3) Journal of Mass Media Ethic 168

Tall N, ‘DPP interim guidelines on prosecuting cases involving communications sent via social media - a matter of common sense?’ (2013) 24(3) Entertainment Law Review 88

Virgo G, ‘Part 2 of the Serious Crime Act 2007 - enough is enough’ (2013) 3 Archbold Review 7

Wasik M, ‘Law reform proposals on computer misuse’ (1989) Apr Criminal Law Review 257

Online Journals

Bocij P, ‘Victims of Cyberstalking: An Exploratory Study of Harassment Perpetrated via the Internet’ (2003) 8(10) First Monday <http://firstmonday.org/ojs/index.php/fm/article/view/1086>

Dorfman R, ‘Can you say “social media prosecutions” with a straight face? The Crown Prosecution Service can’ (2013) The Leeds Journal of Law and Criminology <http://criminology.leeds.ac.uk/2013/09/05/social-media-prosecutions/>

Dyson E, Gilder G, Keyworth G & Toffler A, ‘Cyberspace and the American Dream: A Magna Carta for the Knowledge Age’ (1994) Future Insight <http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html>

Gleeson J, ‘“(Not) working 9–5”: the consequences of contemporary Australian-based online feminist campaigns as digital labour’ (2016) 16(1) Media International

Australia 77 <http://journals.sagepub.com/doi/pdf/10.1177/1329878X16664999>

Halder D & Jaishankar K, 'Cyber Socializing and Victimization of Women' (2009) TEMIDA 5 <http://www.doiserbia.nb.rs/img/doi/1450-6637/2009/1450-66370903005H.pdf>

Karusala N, Bhalla A & Kumah N, Privacy, Patriarchy, and Participation on Social Media (2019) <https://static1.squarespace.com/static/59f549a3b7411c736b42936a/t/5cc217ed1464540001305a53/1556223981510/DIS2019.pdf>

John A *et al*, Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review (2018) 20(4) J Med Internet Res <https://www.jmir.org/2018/4/e129/>

Pegg S, 'Wrong on "revenge porn"' (2015) The Law Society Gazette <https://www.lawgazette.co.uk/comment-and-opinion/wrong-on-revenge-porn/5046957.article>

Thesis

Bates S, '"Stripped": An Analysis of Revenge Porn Victims' Lives after Victimization' (Master of Arts Thesis, Simon Fraser University 2015)

Powell-Jones H, 'How do young people interpret and construct risk in an online context?' (PhD Thesis, City London University 2018)

Hansard

HC Deb 12 December 2018, vol 651, col 277

HC Deb 19 June 2014, vol 582, col 1368

HC Deb 16 May 2012, vol 545, col 175

HC Deb 12 December 2000, vol 359, col 481

HL Deb 24 January 1997, vol 1, col 917

HC Deb 9 February 1990, vol 166, col 1134

HC Deb 12 February 1988, vol 127, col 615

HC Deb 13 January 1986, vol 89, col 792

Reports

Amnesty International:

'Toxic Twitter- A Toxic Place For Women' (*Amnesty International*, 2017) <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/>

'Amnesty reveals alarming impact of online abuse against women' (*Amnesty International*, 20 November 2017) <https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/>

‘Black and Asian women MPs abused more online’ (*Amnesty International*, 2017) <https://www.amnesty.org.uk/online-violence-women-mps>

‘Online abuse of women widespread in UK’ (*Amnesty International*, 2017) <https://www.amnesty.org.uk/online-abuse-women-widespread>

ARTICLE 19, ‘Germany: The Act to Improve Enforcement of the Law in Social Networks’ (*article19.org*, August 2017) <https://www.article19.org/wp-content/uploads/2017/09/170901-Legal-Analysis-German-NetzDG-Act.pdf>

Baber M & Jeffs H, Stalking, harassment and intimidation and the Protection from Harassment Bill (Research Paper 96/115, 13 December 1996)

Brown A, Maple C & Short E, ‘Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey’ (*University of Bedfordshire National Centre for Cyberstalking Research*, 2011) <https://www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf>

Children’s Commissioner, ‘Growing Up Digital: A reports of the Growing Up Digital Taskforce’ (*Children’s Commissioner*, January 2017) <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf>

Clarke R, *Tackling Vandalism* (Home Office Research Study 47, 1978)

Commission:

‘Tackling Illegal Content Online: Towards an enhanced responsibility of online platforms’ COM (2017) 55 final

‘European Strategy for a Better Internet for Children’ COM (2012) 196 final

Committee on Standards in Public Life, *Intimidation in Public Life: A Review by the Committee on Standards in Public Life* (HC 2017-18)

Communications Committee

Regulating in a digital world (HL 2017-19, 299)

Social Media and Criminal Offences (HL 2014-15, 37)

Criminal Justice Inspectorates & HM Crown Prosecution Service Inspectorate, ‘Living in fear – the police and CPS response to harassment and stalking’ (*justiceinspectorates.gov*, July 2017) <http://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/living-in-fear-the-police-and-cps-response-to-harassment-and-stalking.pdf>

Datta B *et al*, ‘Guavas and Genital: A research study in Section 67 of the Information Technology Act’ (*Point of View*, 2017) <https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Smita_Vanniyar.pdf>

Department for Digital, Culture, Media & Sport and Leveson Inquiry, ‘Leveson Inquiry - Report into the culture, practices and ethics of the press’ (*Gov.uk*, 29 November 2012) <https://www.gov.uk/government/publications/leveson-inquiry-report-into-the-culture-practices-and-ethics-of-the-press>

Digital, Culture, Media & Sport Committee, *Disinformation and "fake news": Interim Report* (HC 2017-179 363)

Ditch the Label:

'The Annual Bullying Survey 2018' (*Ditch the Label*, 2018) <https://www.ditchthelabel.org/wp-content/uploads/2018/06/The-Annual-Bullying-Survey-2018-2.pdf>

'The Annual Bullying Survey 2017' (*Ditch the Label*, 2017) <https://www.ditchthelabel.org/wp-content/ uploads/2017/07/The-Annual-Bullying-Survey-2017-2.pdf>

'The Annual Bullying Survey 2016' (*Ditch the Label*, 2016) <http://www.ditchthelabel.org/wp-content/uploads/2016/04/Annual-Bullying-Survey-2016-Digital.pdf >

'The Annual Bullying Survey 2015' (*Ditch the Label*, 2015) <http://ditchthelabel.org/downloads/abs2015.pdf>

HM Government:

Online Harms White Paper (CP 57, 2019)

'Government response to the Internet Safety Strategy Green Paper' (*Gov.uk,* May 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf >

Serious and Organised Crime Strategy (CM 8715, 2013)

Home Affairs Committee:

Oral Evidence: Hate Crime and its Violent Consequences (HC 2017, 609)

Hate crime: abuse, hate and extremism online (HC 2016-17, 609)

Home Office

New Powers Against Organised and Financial Crime (CM 6875, July 2006)

One Step Ahead: A 21st Century Strategy to Defeat Organised Crime (CM 6167, 2004)

Stalking A Consultation Paper (11 July 1996)

The Protection from Harassment Act 1997: Improving Protection for Victims of Stalking (2012)

Judge Theodor Meron, *The Principle of Legality in International Criminal Law* (Legal Studies Research Papers Series 10-08, 2010)

La Rue F, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (*Human Rights Council*, 16 May 2011) <https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>

Law Commission:

Abusive and Offensive Online Communications: A Scoping Report (Law Com No 381, 2018)

Inchoate liability for assisting and encouraging crime (Law Com No 6878, 2006)

Adult Social Care (Law Com No 326, 1995)

Criminal Law: Computer Misuse (Law Com No 1986, 1989)

Report on Poison-Pen Letters (Law Com No 147, 1985)

Parliament of Australia, *Cyber Safety - Joint Select Committee High-wire act: Cyber-safety and the young Interim report* (June 2011)

Petitions Committee, *Oral evidence: Online abuse and the experience of disabled people* (HC 2017, 759)

Robinson D, *The Principle of Legality in International Criminal Law* (Legal Studies Research Papers Series 10-08, 2010)

Schaack B V, *The Principle of Legality in International Criminal Law* (Legal Studies Research Papers Series 10-08, 2010)

Select Committee on Communications, *Growing up with the internet* (HL 2016-17, 130)

The Children's Society, 'Safety Net: Cyberbullying's impact on young people's mental health Inquiry report' (*The Children's Society*, 2018) <https://www.childrenssociety.org.uk/sites/default/files/social-media-cyberbullying-inquiry-full-report_0.pdf>

The Crown Prosecution Service, 'Violence against women and girls report: tenth edition' (*CPS.gov*, 2017) <https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2017.pdf>

United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime-Draft* (United Nations, February 2013)

Conference Papers

Golumbia D, 'Cyberlibertarianism: The Extremist Foundations of "Digital Freedom"' (Clemson University, South Carolina, September 2013)

Newspaper Articles

AAP, 'Revenge porn bill passes Australian Senate' *news.com.au* (Sydney, 15 February 2018) <https://www.news.com.au/technology/online/revenge-porn-bill-passes-australian-senate/news-story/d911487ff7aa8b109f518d7ca0d72aa1>

Akwagyiram A, 'England riots: One year on' *The BBC* (London, 6 August 2012) <http://www.bbc.co.uk/news/uk-19077349>

Ankel S, 'Many revenge porn victims consider suicide – why aren't schools doing more to stop it?' *The Guardian* (London, 7 May 2018) <https://www.theguardian.com/lifeandstyle/2018/may/07/many-revenge-porn-victims-consider-suicide-why-arent-schools-doing-more-to-stop-it>

Barrett D:

‘Faking social media accounts could lead to criminal charges’ *The Telegraph* (London, 3 March 2016) <https://www.telegraph.co.uk/news/uknews/crime/12180782/Faking-social-media-accounts-could-lead-to-criminal-charges.html>

‘Police “dismissive” of online crime, finds watchdog’ *The Telegraph* (London, 22 December 2015) <http://www.telegraph.co.uk/news/uknews/crime/12064353/Police-dismissive-of-online-crime-finds-watchdog.html>

BBC Sport, ‘Bolton's Fabrice Muamba collapses during Spurs-Bolton match’ *The BBC* (London, 17 March 2012) <http://www.bbc.co.uk/sport/football/17417973>

Beckford M, ‘London riots: Almost 1,000 jailed as judges give tougher sentences’ *The Telegraph* (London, 22 February 2012) <http://www.telegraph.co.uk/news/uknews/crime/9101436/London-riots-Almost-1000-jailed-as-judges-give-tougher-sentences.html>

Bliss L:

‘What Facebook isn’t telling us about its fight against online abuse’ *The Conversation* (London, 21 May 2018) <https://theconversation.com/what-facebook-isnt-telling-us-about-its-fight-against-online-abuse-96818>

‘Abuse of women MPs is not just a scandal – it’s a threat to democracy’ *The Conversation* (London, 17 July 2017) <https://theconversation.com/abuse-of-women-mps-is-not-just-a-scandal-its-a-threat-to-democracy-80781>

Boffey D, ‘EU threatens to crack down on Facebook over hate speech’ *The Independent* (London, 11 April 2011) <https://www.theguardian.com/technology/2018/apr/11/eu-heavy-sanctions-online-hate-speech-facebook-scandal>

Bowcott O, Siddique H & Sparrow A, ‘Facebook cases trigger criticism of “disproportionate” riot sentences’ *The Guardian* (London, 17 August 2011) <https://www.theguardian.com/uk/2011/aug/17/facebook-cases-criticism-riot-sentences>

Brooks L, ‘Review brings misogyny as a hate crime a step closer’ *The Guardian* (London, 6 September 2018) <https://www.theguardian.com/society/2018/sep/05/first-step-to-misogyny-becoming-a-hate-called-amazing-victory>

Bulman M, ‘Victim of online harassment feels “absolutely hopeless” over police inaction’ *The Telegraph* (London, 6 July 2017) <http://www.independent.co.uk/news/uk/home-news/online-harassment-victim-sussex-police-inaction-absolutely-hopeless-a7825691.html>

Cadwalladr C & Graham-Harrison E, ‘Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’ *The Guardian* (London, 17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

Cain S, ‘Nearly 130 public libraries closed across Britain in the last year’ *The Guardian* (London, 7 December 2018) <https://www.theguardian.com/books/2018/dec/07/nearly-130-public-libraries-closed-across-britain-in-the-last-year>

Chakelian A, ‘Facebook releases Brexit campaign ads for the fake news inquiry – but what’s wrong with them?’ *NewStateman* (London, 27 July 2018) <https://www.newstatesman.com/politics/media/2018/07/facebook-releases-brexit-campaign-ads-fake-news-inquiry-what-s-wrong-them>

Chishti S, ‘Prescription post Section 66A: “Change law to punish hate speech online”’ *The Indian Express* (New Delhi, 6 October 2017) <https://indianexpress.com/article/india/hate-speech-online-punishment-supreme-court-section-66a-information-technology-act-narendra-modi-4876648/>

Choney S, ‘“Revenge porn” law in California could pave way for rest of nation’ *NBC News* (New York, 3 September 2013) <https://www.nbcnews.com/technolog/revenge-porn-law-california-could-pave-way-rest-nation-8C11022538>

Cohen C, ‘Twitter trolls: The celebrities who’ve been driven off social media by abuse’ *The Telegraph* (London, 18 November 2014) <https://www.telegraph.co.uk/women/womens-life/11238018/Celebrity-Twitter-trolls-The-famous-people-whove-been-driven-off-social-media-by-abuse.html>

Cohen N, ‘“Twitter joke” case only went ahead at insistence of DPP’ *The Guardian* (London, 28 July 2012) <https://www.theguardian.com/law/2012/jul/29/paul-chambers-twitter-joke-airport>

Constine J:

> ‘Facebook and Instagram change to crack down on underage children’ (*Tech Crunch*, 2018) <https://techcrunch.com/2018/07/19/facebok-under-13/>
>
> ‘Facebook now has 2 billion monthly users … and responsibility’ (*Tech Crunch*, 2017) <https://techcrunch.com/2017/06/27/facebook-2-billion-users/>

Cook E, ‘Harassed relentlessly by a stranger, Evonne von Heussen formed an anti-stalking group. Emma Cook reports’ *The Independent* (London, 22 January 1995) <http://www.independent.co.uk/life-style/stalked-for-years-by-a-man-she-met-once-1569160.html>

Cuthbertson A, ‘Facebook knew about Cambridge Analytica data breach a year before Trump election’ *The Independent* (London, 6 April 2018) <https://www.independent.co.uk/news/business/news/facebook-cambridge-analytica-trump-election-data-breach-mark-zuckerberg-a8292071.html>

Davey M, ‘Online sexism targeted in world-first “bystander” project’ *The Guardian* (London, 31 May 2018) <https://www.theguardian.com/world/2018/jun/01/online-sexism-targeted-in-world-first-bystander-project>

Davies C:

> ‘One-quarter of Britons witnessed hate speech in past year, poll finds’ *The Guardian* (London, 27 January 2018) <https://www.theguardian.com/society/2018/jan/27/uk-hate-speech-poll-holocaust-memorial-day-2018>
>
> ‘Katie Price urges MPs to act after “horrific” online abuse of son’ *The Guardian* (London, 6 February 2018)

<https://www.theguardian.com/media/2018/feb/06/katie-price-urges-mps-to-make-online-abuse-a-criminal-offence>

Dearden L, 'Germany to fine social networks up to €50m for not taking down illegal "fake news" posts' *The Independent* (London, 5 April 2017) <https://www.independent.co.uk/news/world/europe/germany-fake-news-social-networks-fine-facebook-50-million-euros-illegal-content-hate-speech-angela-a7668731.html>

Ditum S, 'If the law actually worked, Joshua Stimpson wouldn't have been able to stab Molly McLaren 75 times in broad daylight' *The Independent* (London,7 February 2018) <https://www.independent.co.uk/voices/molly-mclaren-stalking-joshua-stimpson-stabbed-theodore-johnson-cps-a8198836.html>

Dodd V & Davies C, 'London riots escalate as police battle for control' *The Guardian* (London, 9 August 2011) <https://www.theguardian.com/uk/2011/aug/08/london-riots-escalate-police-battle>

Dowell B, 'Mary Beard suffers "truly vile" online abuse after Question Time' *The Guardian* (London, 21 January 2013) <https://www.theguardian.com/media/2013/jan/21/mary-beard-suffers-twitter-abuse>

D'Urso J, 'Who spent what on Facebook during 2017 election campaign?' *The BBC* (London, 31 March 2018) <https://www.bbc.co.uk/news/uk-politics-43487301>

Elgot J, 'Diane Abbott more abused than any other MPs during election' *The Guardian* (London, 5 September 2017) <https://www.theguardian.com/politics/2017/sep/05/diane-abbott-more-abused-than-any-other-mps-during-election>

Evans P, 'Will Germany's new law kill free speech online?' *The BBC* (London,18 September 2017) <https://www.bbc.co.uk/news/blogs-trending-41042266>

Fention S, 'Revenge porn laws: First person found guilty under new laws to be sentenced today' *The Independent* (London, 7 August 2015) <http://www.independent.co.uk/news/uk/crime/revenge-porn-laws-first-person-found-guilty-under-new-laws-to-be-sentenced-today-10444898.html>

Fifield N, 'Cyber stalker bugged women's computers to spy on them in their bedrooms' *The Telegraph* (London, 30 May 2014) <http://www.telegraph.co.uk/news/uknews/crime/10866262/Cyber-stalker-bugged-womens-computers-to-spy-on-them-in-their-bedrooms.html>

Fox C, 'What is Article 13? The EU's copyright directive explained' *The BBC* (London, 14 February 2019) <https://www.bbc.co.uk/news/technology-47239600

Green D A, 'The "Twitter Joke Trial" returns to the High Court' *NewStatesman* (London, 22 June 2012) <https://www.newstatesman.com/blogs/david-allen-green/2012/06/twitter-joke-trial-david-allen-green>

Greenfield P, 'The Cambridge Analytica files: the story so far' *The Guardian* (London, 26 March 2018) <https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far>

Gregory J, 'Aristocrat faces jail after being menacing and racist about Gina Miller' *The Guardian* (London, 11 July 2017) <https://www.theguardian.com/uk-

news/2017/jul/11/man-jail-offering-moneyrun-over-gina-miller-rhodri-philipps-viscount-brexit>

Halliday J, 'Helen Skelton quits Twitter after abuse from trolls' *The Guardian* (London, 2 August 2012) <https://www.theguardian.com/technology/2012/aug/02/celebrities-quit-twitter-abuse>

Hamilton F, 'Police wait 18 months for evidence from social media firms' *The Times* (London, 14 September 2018) <https://www.thetimes.co.uk/article/police-wait-18-months-for-evidence-from-social-media-firms-6djhnwcj0>

Hards S, 'The Penlee Lifeboat disaster happened 36 years ago today - we remember the heroes of the Solomon Browne' *CornwallLive* (Truro, 19 December 2017) <https://www.cornwalllive.com/news/cornwall-news/penlee-lifeboat-disaster-happened-36-945008>

Harkin G, 'Family devastated after tragic Erin (13) takes own life after vicious online bullying' *Irish Independent* (Dublin, 29 October 2012) <https://www.independent.ie/irish-news/family-devastated-after-tragic-erin-13-takes-own-life-after-vicious-online-bullying-28824852.html>

Hattenstone S, 'Caroline Criado-Perez: '"Twitter has enabled people to behave in a way they wouldn't face to face"' *The Guardian* (London, 4 August 2013) <https://www.theguardian.com/lifeandstyle/2013/aug/04/caroline-criado-perez-twitter-rape-threats>

Hayden S, 'Labour's Jess Phillips received "600 rape and death threats in a single day"' *The Independent* (London, 27 August 2017) <http://www.independent.co.uk/news/uk/home-news/labour-mp-jess-phillips-rape-death-threats-one-day-social-media-attacks-training-a7915406.html>

Heath A, 'Twitter outlines how it will be tougher on banning revenge porn' *Business Insider UK* (London, 27 October 2017) <https://www.businessinsider.com/twitter-tougher-revenge-porn-backlash-2017-10?r=UK>

Hern A:

> 'Why won't Facebook give access to Lucy McHugh murder suspect's account?' *The Guardian* (London, 5 September 2018) <https://www.theguardian.com/uk-news/2018/sep/05/why-wont-facebook-provide-access-lucy-mchugh-suspect-account>
>
> 'Twitter further tightens abuse rules in attempt to prove it cares' *The Guardian* (London, 18 October 2017) <https://www.theguardian.com/technology/2017/oct/18/twitter-abuse-rules-jack-dorsey-hate-speech-revenge-porn-violent-groups-social-network>

Higgens D, 'Man jailed for riot race-hate posts' *The Independent* (London, 4 November 2011) <http://www.independent.co.uk/news/uk/crime/man-jailed-for-riot-race-hate-posts-6257282.html>

Hopkins N:

> 'How Facebook allows users to post footage of children being bullied' *The Guardian* (London, 22 May 2017) <https://www.theguardian.com/news/2017/may/22/how-facebook-allows-users-to-post-footage-of-children-being-bullied>

‘Facebook moderators: a quick guide to their job and its challenges’ *The Guardian* (London, 21 May 2017) <https://www.theguardian.com/news/2017/may/21/facebook-moderators-quick-guide-job-challenges>

‘Revealed: Facebook's internal rulebook on sex, terrorism and violence’ *The Guardian* (London, 21 May 2017) <https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence>

Hopkins N & Solon O, ‘Facebook flooded with “sextortion” and “revenge porn”, files reveal’ *The Guardian* (London, 22 May 2017) <https://www.theguardian.com/news/2017/may/22/facebook-flooded-with-sextortion-and-revenge-porn-files-reveal>

Hopkins N & Wong J C, ‘Has Facebook become a forum for misogyny and racism?’ *The Guardian* (London, 21 May 2017) <https://www.theguardian.com/news/2017/may/21/has-facebook-become-forum-misogyny-racism>

Horman R, ‘We have a stalking law – so why don’t the police use it?’ *The Guardian* (London, 19 August 2016) <https://www.theguardian.com/commentisfree/2016/apr/19/stalking-law-police-lily-allen-stalked-criminal-justice-system>

Huber A R, ‘Revenge porn law is failing victims – here’s why’ *The Conversation* (London, 25 January 2018) <https://theconversation.com/revenge-porn-law-is-failing-victims-heres-why-90497>

ITV News:

‘Blogger “mocked Anne Frank and Holocaust survivors” court told’ *ITV News* (London, 11 January 2018) <http://www.itv.com/news/2018-01-11/blogger-mocked-anne-frank-and-holocaust-survivors-court-told/>

‘Student who sent “vile” tweets to murdered James Bulger’s mother jailed for three years’ *ITV News* (London, 14 July 2016) <http://www.itv.com/news/2016-07-14/student-who-sent-vile-tweets-to-murdered-james-bulgers-mother-jailed-for-three-years/>

Jacobs H, ‘This is what it is like to be the victim of revenge porn, and why we need to criminalise it’ *The Telegraph* (London, 13 February 2015) <http://www.independent.co.uk/voices/comment/this-is-what-it-is-like-to-be-the-victim-of-revenge-porn-and-why-we-need-to-criminalise-it-10045067.html>

Jeavans C, ‘The miners’ darkest year’ *The BBC* (London, 4 March 2004) <http://news.bbc.co.uk/1/hi/uk/3494024.stm>

Karp P, ‘Australia passes social media law penalising platforms for violent content’ *The Guardian* (London, 4 April 2019) <https://www.theguardian.com/media/2019/apr/04/australia-passes-social-media-law-penalising-platforms-for-violent-content?CMP=share_btn_tw>

Khomami N, ‘NSPCC records 88% rise in children seeking help for online abuse’ *The Guardian* (London, 14 November 2016) <https://www.theguardian.com/society/2016/nov/14/nspcc-records-88-rise-in-children-seeking-help-for-online-abuse>

Kleinman Z, ‘Article 13: Memes exempt as EU backs controversial copyright law’ *The BBC* (London, 26 March 2019) <https://www.bbc.co.uk/news/technology-47708144>

Knapton S, ‘Cyberbullying makes young people twice as likely to self harm or attempt suicide’ *The Telegraph* (London, 22 April 2018) <https://www.telegraph.co.uk/science/2018/04/22/cyberbullying-makes-young-people-twice-likely-self-harm-attempt/>

Laville S:

> ‘Internet troll who sent labour MP antisemitic abused is jailed’ *The Guardian* (London, 10 February 2017) <https://www.theguardian.com/uk-news/2017/feb/10/internet-troll-who-sent-labour-mp-antisemitic-messages-is-jailed>
>
> ‘Online abuse: “existing laws too fragmented and don’t serve victims”’ *The Guardian* (London, 4 March 2016) <https://www.theguardian.com/uk-news/2016/mar/04/online-abuse-existing-laws-too-fragmented-and-dont-serve-victims-says-police-chief>
>
> ‘“Revenge Porn” victims should get anonymity, say 75% of people’ *The Guardian* (London, 19 July 2016) <https://www.theguardian.com/law/2016/jul/19/revenge-porn-victims-should-get-anonymity-say-75-per-cent-of-people>

Lee B, ‘Sharing our stories is the strength at the heart of #MeToo. We must repeal gag laws’ *The Guardian* (London, 19 November 2018) <https://www.theguardian.com/commentisfree/2018/nov/19/sharing-our-stories-is-the-strength-at-the-heart-of-metoo-we-must-repeal-gag-laws>

Lee D, ‘Facebook details scale of abuse on its site’ *The BBC* (London, 15 May 2018) <http://www.bbc.co.uk/news/technology-44122967>

Levin S, ‘Facebook temporarily blocks Black Lives Matter activist after he posts racist email’ *The Guardian* (London, 12 September 2016) <https://www.theguardian.com/technology/2016/sep/12/facebook-blocks-shaun-king-black-lives-matter>

Lochlainn GMN, ‘Facebook data harvesting: what you need to know’ *The Conversation* (London, 3 April 2018) <http://theconversation.com/facebook-data-harvesting-what-you-need-to-know-93959>

MacDonald K, ‘Parents: don't panic about Momo - worry about YouTube Kids instead’ *The Guardian* (London, 28 February 2019) <https://www.theguardian.com/commentisfree/2019/feb/28/parents-momo-scare-youtube-kids>

Madrigal A C, ‘A Belgian Legislator Berates and Scoffs at Mark Zuckerberg’ *The Atlantic* (Boston, 22 May 2018) <https://www.theatlantic.com/technology/archive/2018/05/a-belgian-legislator-berates-and-scoffs-at-mark-zuckerberg/560960/>

Marsh S, ‘Surge in crimes against MPs sparks fears over intimidation and abuse’ *The Guardian* (London, 23 October 2018) <https://www.theguardian.com/politics/2018/oct/23/crimes-mps-uk-online-intimidation-abuse>

Mason R, ‘Diane Abbott on abuse of MPs: “My staff try not to let me go out alone”’ *The Guardian* (London, 19 February 2017) <https://www.theguardian.com/politics/2017/feb/19/diane-abbott-on-abuse-of-mps-staff-try-not-to-let-me-walk-around-alone>

McCann K, ‘Social media giants should be forced to pay for policing social media, report backed by Amber Rudd claims’ *The Telegraph* (London, 1 May 2017) <https://www.telegraph.co.uk/news/2017/04/30/social-media-giants-should-forced-pay-policing-social-media/>

McSmith A, ‘Tough riot sentences prompt new guidelines for the courts’ *The Independent* (London, 17 August 2011) <http://www.independent.co.uk/news/uk/crime/tough-riot-sentences-prompt-new-guidelines-for-the-courts-2339699.html>

Moore B, ‘Facebook internet “troll” Sean Duffy jailed’ *The BBC* (London, 13 September 2011) <http://www.bbc.co.uk/news/av/uk-england-14907590/facebook-internet-troll-sean-duffy-jailed>

Morris S & Sabbagh D, ‘April Jones: Matthew Woods jailed over explicit Facebook comments’ *The Guardian* (London, 8 October 2012) <https://www.theguardian.com/uk/2012/oct/08/april-jones-matthew-woods-jailed>

Morris S:

> ‘Student jailed for racist Fabrice Muamba tweets’ *The Guardian* (London, 27 March 2012) <https://www.theguardian.com/uk/2012/mar/27/student-jailed-fabrice-muamba-tweets>
>
> ‘Internet troll jailed after mocking deaths of teenagers’ *The Guardian* (London, 13 September 2011) <https://www.theguardian.com/uk/2011/sep/13/internet-troll-jailed-mocking-teenagers>

Murgia M, ‘The world's first website went online 25 years ago today’ *The Telegraph* (London, 21 December 2015) <https://www.telegraph.co.uk/technology/internet/12061803/The-worlds-first-website-went-online-25-years-ago-today.html>

Narayan V, ‘Man booked under IT Act for “defaming” CM Devendra Fadnavis’ *The Times of India* (Mumbai, 10 July 2015) <https://timesofindia.indiatimes.com/india/Man-booked-under-IT-Act-for-defaming-CM-Devendra-Fadnavis-in-tweet/articleshow/48011122.cms>

Nasr J, ‘Beatrix von Storch: German police accuse AfD politician of hate incitement over anti-Muslim tweet’ *The Independent* (London, 2 January 2018) <https://www.independent.co.uk/news/world/europe/beatrix-von-storch-germany-afd-anti-muslim-twitter-north-rhine-westphalia-new-years-eve-a8138086.html>

O’Carroll L, ‘Gina Miller: “I’ve been told that as a colored women, I’m not even human”’ *The Guardian* (London, 25 January 2017) <https://www.theguardian.com/politics/2017/jan/25/parliament-alone-issovereign-gina-miller-speaks-out-after-article-50-victory>

Oltermann P, ‘Tough new German law puts tech firms and free speech in spotlight’ *The Guardian* (London, 5 January 2018) <https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-

firms-and-free-speech-in-spotlight>

O'Malley K, 'What Is Upskirting And When Did It Become A Criminal Offence?' *The Independent* (London, 12 April 2019) <https://www.independent.co.uk/life-style/women/upskirting-illegal-definition-crime-uk-sexual-harassment-a8864636.html>

Parry G, Tirbutt S & Rose D, 'From the archive: Riots in Brixton after police shooting' *The Guardian* (London, 30 September 1985) <https://www.theguardian.com/theguardian/2009/sep/30/brixton-riots-1985-archive>

Perry K, 'Revenge porn: some of the biggest celebrity victims' *The Telegraph* (London, 30 September 2014) <http://www.telegraph.co.uk/news/celebritynews/11129357/Revenge-porn-some-of-the-biggest-celebrity-victims.html>

Phillips S, 'A brief history of Facebook' *The Guardian* (London, 25 July 2007) <https://www.theguardian.com/technology/2007/jul/25/media.newmedia>

Pilkington E, 'Justine Sacco, PR executive fired over racist tweet, "ashamed"' *The Guardian* (London, 22 December 2013) <https://www.theguardian.com/world/2013/dec/22/pr-exec-fired-racist-tweet-aids-africa-apology>

Powell A, Flynn A & Henry N, 'FactCheck Q&A: are there laws to protect against "revenge porn" in Australia?' *The Conversation* (London, 8 March 2017) <https://theconversation.com/factcheck-qanda-are-there-laws-to-protect-against-revenge-porn-in-australia-74154>

Powell-Jones H, 'Online abuse: teenagers might not report it because they often don't see it as a problem' *The Conversation* (London, 7 May 2019) <https://theconversation.com/online-abuse-teenagers-might-not-report-it-because-they-often-dont-see-it-as-a-problem-116479>

Press Association:

> 'Social media-related crime reports up 780% in four years' *The Guardian* (London, 27 December 2012) <https://www.theguardian.com/media/2012/dec/27/social-media-crime-facebook-twitter>
>
> 'Britain's Got Talent blogger cautioned by police' *The Guardian* (London, 3 July 2011) <https://www.theguardian.com/tv-and-radio/2011/jul/03/britains-got-talent-blogger-cautioned> accessed 1 May 2018

Rankin J, 'Tech firms could face new EU regulations over fake news' *The Guardian* (London, 24 April 2018) <https://www.theguardian.com/media/2018/apr/24/eu-to-warn-social-media-firms-over-fake-news-and-data-mining>

Rawlinson K, 'Twitter faces boycott after "inaction" over rape threats against feminist bank notes campaigner Caroline Criado-Perez' *The Independent* (London, 27 July 2013) <https://www.independent.co.uk/news/uk/home-news/twitter-faces-boycott-after-inaction-over-rape-threats-against-feminist-bank-notes-campaigner-8734856.html>

Rayner G & McCann K, 'Twitter is "failing women" by taking too long to remove misogynistic abuse, Yvette Cooper says' *The Telegraph* (London, 22 August 2017)

<https://www.telegraph.co.uk/news/2017/08/21/twitter-failing-women-taking-long-remove-misogynistic-abuse/>

Roberts R, 'Online hate crime to be tackled by new national police hub, Home Secretary says' *The Independent* (London, 8 October 2017) <https://www.independent.co.uk/news/uk/politics/online-hate-crime-amber-rudd-home-office-national-police-hub-facebook-twitter-trolls-a7988411.html>

Robinson B & Dowling N, 'Revenge porn laws "not working", says victims group' *The BBC* (London, 19 May 2019) <https://www.bbc.co.uk/news/uk-48309752>

Ronson J, 'How One Stupid Tweet Blew Up Justine Sacco's Life' *The New York Times Magazine* (New York, 12 February 2015) <https://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html> accessed 5 February 2019

Saunders A, 'Hate is hate. Online abusers must be dealt with harshly' *The Guardian* (London, 21 August 2017) <https://www.theguardian.com/commentisfree/2017/aug/20/hate-crimes-online-abusers-prosecutors-serious-crackdown-internet-face-to-face>

Sherlock P, 'Revenge pornography victims as young as 11, investigation finds' *The BBC* (London, 27 April 2016) <http://www.bbc.co.uk/news/uk-england-36054273>

Sims A, 'Trolling, Abuse, Sexting and Doxxing all targeted in ambitious new legal guidelines' *The Independent* (London, 10 October 2016) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/online-abuse-internet-sexting-doxxing-trolling-new-legal-guidelines-crime-prosecution-service-a7353536.html>

Solon O:

> 'Facebook posts record revenues for first quarter despite privacy scandal' *The Guardian* (London, 25 April 2018) <https://www.theguardian.com/technology/2018/apr/25/facebook-first-quarter-2018-revenues-zuckerberg>
>
> 'Underpaid and overburdened: the life of a Facebook moderator' *The Guardian* (London, 25 May 2017) <https://www.theguardian.com/news/2017/may/25/facebook-moderator-underpaid-overburdened-extreme-content>

Southworth P, 'Parents warned about 'Momo' suicide game on YouTube' *The Telegraph* (London, 27 February 2019) <https://www.telegraph.co.uk/news/2019/02/27/parents-warned-online-suicide-game-appearing-peppa-pig-videos/>

Sparrow A, 'David Cameron announces recall of parliament over riots' *The Guardian* (London, 9 August 2011) <https://www.theguardian.com/uk/2011/aug/09/david-cameron-announces-recall-parliament>

Stuart K, 'Zoe Quinn: "All Gamergate has done is ruin people's lives"' *The Guardian* (London, 3 December 2014) <https://www.theguardian.com/technology/2014/dec/03/zoe-quinn-gamergate-interview>

Sweney M, ‘Is Facebook for old people? Over-55s flock in as the young leave’ *The Guardian* (London, 12 February 2018) <https://www.theguardian.com/technology/2018/feb/12/is-facebook-for-old-people-over-55s-flock-in-as-the-young-leave>

Telegraph Reporters, ‘What happened to murdered April Jones and who is Mark Bridger?’ *The Telegraph* (London, 20 June 2017) <https://www.telegraph.co.uk/news/0/happened-murdered-april-jones-mark-bridger/>

The BBC:

‘Facebook: New Zealand attack video viewed 4,000 times’ *The BBC* (London, 19 March 2019) <https://www.bbc.co.uk/news/business-47620519>

‘Lucy McHugh death: “Challenge” over accessing Facebook information’ *The BBC* (London, 4 September 2018) <https://www.bbc.co.uk/news/uk-england-hampshire-45408338>

‘Facebook wants your naked photos to stop revenge porn’ *The BBC* (London, 23 May 2018) <https://www.bbc.co.uk/news/newsbeat-44223809>

‘Hate crime “police priority” as social media cases soar’ *The BBC* (London, 17 March 20180 <https://www.bbc.co.uk/news/uk-scotland-glasgow-west-43436900

‘Cyberbullying and trolling reports to Welsh police double’ *The BBC* (London, 24 October 2017) <https://www.bbc.co.uk/news/uk-wales-41729206>

‘Teenager's life “ruined” by Live.me and Twitter “trolls”’ *The BBC* (London, 24 October 2017) <http://www.bbc.co.uk/news/uk-england-41693437>

‘On this day: 1985: Riots in Brixton after police shooting’ *The BBC* (London, 2017) <http://news.bbc.co.uk/onthisday/hi/dates/stories/september/28/newsid_2540000/2540397.stm>

‘Revenge porn: More than 200 prosecuted under new law’ *The BBC* (London, 6 September 2016) <http://www.bbc.co.uk/news/uk-37278264>

‘Nottinghamshire Police records misogyny as a hate crime’ *The BBC* (London, 13 July 2016) <https://www.bbc.co.uk/news/uk-england-nottinghamshire-36775398>

‘Wallasey man jailed for posting “revenge porn” images’ *The BBC* (London, 19 August 2015) <http://www.bbc.co.uk/news/uk-england-merseyside-33992110>

‘Cardiff man sentenced for “revenge porn” post’ *The BBC* (London, 6 July 2015) <http://www.bbc.co.uk/news/uk-wales-south-east-wales-33414500>

‘Who, what, why: What laws currently cover trolling?’ *The BBC* (London, 20 October 2014) <https://www.bbc.co.uk/news/blogs-magazine-monitor-29686865>

‘What caused the 1985 Tottenham Broadwater Farm riot?’ *The BBC* (London, 3 March 2014) <http://www.bbc.co.uk/news/uk-england-london-26362633>

‘Caroline Criado-Perez Twitter abuse case leads to arrest’ *The BBC* (London, 29 July 2013) <https://www.bbc.co.uk/news/uk-23485610>

‘Man fined for Gregory Campbell Facebook comment’ *The BBC* (London, 29 July 2011) <http://www.bbc.co.uk/news/uk-northern-ireland-14345649>

The Guardian:

‘Hate speech and anti-migrant posts: Facebook's rules’ *The Guardian* (London, 24 May 2017) <https://www.theguardian.com/news/gallery/2017/may/24/hate-speech-and-anti-migrant-posts-facebooks-rules>

‘What Facebook says on “sextortion” and “revenge porn”’ *The Guardian* (London, 22 May 2017) <https://www.theguardian.com/news/gallery/2017/may/22/what-facebook-says-on-sextortion-and-revenge-porn>

‘Facebook’s manual on credible threats of violence’ *The Guardian* (London, 21 May 2017) <https://www.theguardian.com/news/gallery/2017/may/21/facebooks-manual-on-credible-threats-of-violence>

The Local, ‘This is what Facebook moderators in Germany have to deal with’ *The Local* (Stockholm, 16 December 2016) <https://www.thelocal.de/20161216/this-is-what-facebook-moderators-in-berlin-have-to-deal-with>

Titcomb J, ‘Facebook admits up to 270m users are fake and duplicate accounts’ *The Telegraph* (London, 2 November 2017) <https://www.telegraph.co.uk/technology/2017/11/02/facebook-admits-270m-users-fake-duplicate-accounts/>

Topping A, ‘Jane Austen Twitter row: two plead guilty to abusive tweets’ *The Guardian* (London, 7 January 2014) <https://www.theguardian.com/society/2014/jan/07/jane-austen-banknote-abusive-tweets-criado-perez>

Townsend M, ‘How the battle of Lewisham helped to halt the rise of Britain’s far right’ *The Guardian* (London, 13 August 2017) <https://www.theguardian.com/uk-news/2017/aug/13/battle-of-lewisham-national-front-1977-far-right-london-police>

Travis A, ‘“Snooper's charter” bill becomes law, extending UK state surveillance’ *The Guardian* (London, 29 November 2016) <https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance>

Urwin R, ‘Half of young women on Facebook suffer abuse’ *The Sunday Times* (London, 2 March 2018) <https://www.thetimes.co.uk/edition/news/half-of-young-women-on-facebook-suffer-abuse-3lxbhhnjj>

Vaidyanathan R, ‘India Facebook arrests: Shaheen and Renu speak out’ *The BBC* (London, 26 November 2012) <https://www.bbc.co.uk/news/world-asia-india-20490823>

Walker P, ‘Tories spent £18.5m on election that cost them majority’ *The Guardian* (London, 19 March 2018) <https://www.theguardian.com/politics/2018/mar/19/electoral-commission-conservatives-spent-lost-majority-2017-election>

Wall D S & Chistyakova Y, ‘How organised crime in the UK has evolved beyond the mafia model’ *The Conversation* (London, 18 May 2015) <https://theconversation.com/how-organised-crime-in-the-uk-has-evolved-beyond-the-mafia-model-40782>

Waterson J, ‘Facebook removed 1.5m videos of New Zealand terror attack in first 24 hours’ *The Guardian* (London, 17 March 2019) <https://www.theguardian.com/world/2019/mar/17/facebook-removed-15m-videos-new-zealand-terror-attack>

Weaver M, ‘Police are inconsistent in tackling online abuse, admits chief constable’ *The Guardian* (London, 14 April 2016) <https://www.theguardian.com/uk-news/2016/apr/14/online-abuse-policeinconsistent-digital-crime-stephen-kavanagh>

Wendling M, ‘Election 2017: Was it Facebook wot swung it?’ *The BBC* (London, 10 June 2017) <https://www.bbc.co.uk/news/blogs-trending-40209711>

Williams C, ‘Twitter refuses to hand member information to police’ *The Telegraph* (London, 29 January 2013) <http://www.telegraph.co.uk/technology/twitter/9834776/Twitter-refuses-to-hand-member-information-to-police.html>

Wilson L, ‘Top prosecutor warns Australia’s revenge porn laws are too weak to properly protect women’ *news.com.au* (Sydney, 10 January 2016) <https://www.news.com.au/technology/online/security/top-prosecutor-warns-australias-revenge-porn-laws-are-too-weak-to-properly-protect-women/news-story/b597b7c0f1b0f76c7b7980ca545b512a>

Withnall A, ‘Grenfell Tower bonfire effigy burning leads to five arrests’ *The Independent* (London, 12 February 2019) <https://www.independent.co.uk/news/uk/crime/grenfell-tower-bonfire-effigy-video-fire-burning-guy-fawkes-november-5-a8619491.html>

Worley W:

> ‘German police “shook heads in disbelief” at Breitbart News reporting of New Year’s Eve events in Dortmund’ *The Guardian* (London, 7 January 2017) <https://www.independent.co.uk/news/world/europe/breitbart-news-dortmund-police-new-years-eve-fake-news-germany-angela-merkel-syrians-refugee-crisis-a7514786.html>
>
> ‘Mother of cyber bullying victim pens heartbreaking open letter in response to his suicide’ *The Independent* (London, 6 October 2016) <https://www.independent.co.uk/news/uk/home-news/mother-open-letter-cyber-bullying-victim-suicide-online-social-media-a7347531.html>

Yates S, ‘“Fake news” – why people believe it and what can be done to counter it’ *The Conversation* (London, 13 December 2016) <https://theconversation.com/fake-news-why-people-believe-it-and-what-can-be-done-to-counter-it-70013>

Websites

Barlow J P, ‘A Declaration of the Independence of Cyberspace’ (*Electronic Frontier Foundation*, 8 February 1996) <https://www.eff.org/cyberspace-independence>

Bates B, ‘Laura Bates: Violence Against Women Online’ (*Amnesty International*, 21 March 2018) <https://www.amnesty.org/en/latest/research/2018/03/laura-bates-online-violence-against-women/>

Bates L, ‘The everyday sexism project’ (*Everydaysexism*, 2019) <https://everydaysexism.com/>

Carmichael A, ‘Better protection for victims of “revenge porn”’ (*alistaircarmichael*, 2016) <http://www.alistaircarmichael.co.uk/amendments_to_crime_and_policing_bill>

Centre for Computing History, ‘1971: First Network Email sent by Ray Tomlinson’ (*Centre for Computing History*, 2016) <http://www.computinghistory.org.uk/det/6116/First-e-mail-sent-by-Ray-Tomlinson/>

Citizens Advice, ‘When can a public authority interfere with your human rights?’ (*Citizens Advice*, 2018) <https://www.citizensadvice.org.uk/law-and-courts/civil-rights/human-rights/when-can-a-public-authority-interfere-with-your-human-rights/>

College of Policing, National Crime Agency and National Police Chief’s Council, ‘Digital Investigation and Intelligence: Policing capabilities for a digital age April 2015’ (*NPCC*, April 2015) <http://www.npcc.police.uk/documents/reports/Digital%20Investigation%20and%20Intelligence%20Policing%20capabilities%20for%20a%20digital%20age%20April%202015.pdf>

Commission:

‘Questions and Answers – European Parliament's vote in favour of modernised rules fit for digital age’ (*European Commission Press Release*, 30 April 2019) <http://europa.eu/rapid/press-release_MEMO-19-1849_en.htm>

‘EC to ban prawn cocktail crisps’ (*Euro Myths*, 16 January 1993) <https://blogs.ec.europa.eu/ECintheUK/ec-to-ban-prawn-cocktail-crips/>

Council of the European Union, ‘EU Guidelines: Freedom of Expression Online and Offline’ (*Europa*, 13 May 2014) <https://ec.europa.eu/digital-single-market/en/news/eu-human-rights-guidelines-freedom-expression-online-and-offline>

Criado-Perez C, ‘A Brief Comment on Peter Nunn, Sentenced Today For Twitter Abuse’ (*Week Women*, 2014) <https://weekwoman.wordpress.com/2014/09/29/a-brief-comment-on-peter-nunn/>

Department of Digital, Culture, Media & Sport, ‘Code of Practice for providers of online social media platforms’ (*Gov.uk*, 12 April 2019) <https://www.gov.uk/government/publications/code-of-practice-for-providers-of-online-social-media-platforms/code-of-practice-for-providers-of-online-social-media-platforms>

Department of Home Affairs, ‘Cybercrime’ (*Australian Government*, 2017) <https://www.homeaffairs.gov.au/about/crime/cybercrime>

Department of the Prime Minister and Cabinet, ‘$100 million to help keep women safe’ (*Australian Government,* 24 September 2015) <https://www.pmc.gov.au/news-centre/office-women/100-million-help-keep-women-safe>

Equality and Human Rights Commission, ‘Article 14: Protection from Discrimination’ (*Equality Human Rights*, 4 May 2016)

<https://www.equalityhumanrights.com/en/human-rights-act/article-14-protection-discrimination>

Europa.eu, 'Regulations, Directives and other acts' (*European Union*, 24 May 2018) <https://europa.eu/european-union/eu-law/legal-acts_en>

Europe Institute for Gender Equality, 'Cyber violence against women and girls' (*Europe Institute for Gender Equality*, 2017) <eige.europa.eu/sites/default/files/.../cyber_violence_against_women_and_girls.pd>

Facebook

'Bullying Prevention Hub' (*Facebook*, 2019) <https://www.facebook.com/safety/bullying>

'Bullying Prevention Hub: Teens' (*Facebook*, 2019) <https://www.facebook.com/safety/bullying/teens>

'Community Standards: Introduction' (*Facebook*, 2019) <https://www.facebook.com/communitystandards/>

'Crises Response' (*Facebook*, 2019) <https://www.facebook.com/about/crisisresponse/>

'Going Live on Facebook' (*Facebook*, 2019) <https://live.fb.com/about/>

'Information for law enforcement authorities' (*Facebook*, 2019) <https://www.facebook.com/safety/groups/law/guidelines/>

'What names are allowed on Facebook?' (*Facebook,* 2019) <https://www.facebook.com/help/112146705538576?helpref=faq_content>

'Community Standards: Adult nudity and sexual activity' (*Facebook*, 2018) <https://www.facebook.com/communitystandards/adult_nudity_sexual_activity>

'Community Standards: Bullying' (*Facebook*, 2018) <https://www.facebook.com/communitystandards/bullying>

'Community Standards: Credible Violence' (*Facebook*, 2018) <https://www.facebook.com/communitystandards/credible_violence>

'Community Standards: Hate Speech' (*Facebook*, 2018) <https://www.facebook.com/communitystandards/hate_speech>

'Government Requests for User Data' (*Facebook*, 2018) <https://transparency.facebook.com/government-data-requests/jan-jun-2018>

'Parents Portal' (*Facebook*, 2018) <https://www.facebook.com/safety/parents>

'Youth Portal' (*Facebook*, 2018) <https://www.facebook.com/safety/youth>

'Create An Account' (*Facebook*, 2017) <https://www.facebook.com/help/345121355559712>

‘Facebook Safety’ (*Facebook*, 6 November 2013) <https://www.facebook.com/fbsafety/posts/today-we-are-launching-the-new-bullying-prevention-hub-offering-important-tools-/600514153319760/>

Facebook Events, ‘Bring people together with Facebook Events’ (*Facebook*, 2016) <https://events.fb.com/#events_landing_hero>

Federal Ministry of Justice and Consumer Protection, ‘Questions and answers: Act to Improve Enforcement of the Law in Social Networks’ (*German Government*, 2017) <https://www.bmjv.de/SharedDocs/FAQ/EN/NetzDG/NetzDG.html>

Grayling C, ‘Press release: New law to tackle revenge porn’ (*Gov.uk*, 12 October 2014) <https://www.gov.uk/government/news/new-law-to-tackle-revenge-porn>

HM Government, ‘Revenge Porn: The Facts’ (*Gov.uk*, 2014) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/405286/revenge-porn-factsheet.pdf>

Holman R, ‘“I’ve had death and rape threats simply for starting the conversation about everyday sexism”’ (*The Debrief*, 30 April 2014) <https://thedebrief.co.uk/news/opinion/ve-death-rape-threats-simply-starting-conversation-everyday-sexism/>

Home Office:

‘Statistical News Release: Hate Crime, England and Wales, 2016/17’ (*Gov.uk,* 17 October 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651851/hate-crime-1617-hosb1717snr.pdf>

‘Circular: a change to the Protection from Harassment Act 1997’ (*Gov.uk*, 16 October 2012) <https://www.gov.uk/government/publications/a-change-to-the-protection-from-harassment-act-1997-introduction-of-two-new-specific-offences-of-stalking>

Instagram, ‘Terms of Use’ (*Instagram*, 2016) <https://help.instagram.com/581066165581870>

Internet Live Stats, ‘Total number of Websites’ (*Internet Live Stats*, 2018) <http://www.internetlivestats.com/total-number-of-websites/>

Jourová V, ‘Code of Conduct on countering illegal hate speech online: One year after’ (*European Commission*, June 2017) <https://ec.europa.eu/newsroom/document.cfm?doc_id=40573>

Justice and Consumers, ‘European Commission and IT Companies announce Code of Conduct on illegal online hate speech’ (*European Commission*, 31 May 2016) <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=31811>

Ministry of Electronics & Information Technology, ‘Information Technology Act 2000’ (*Government of India*, 2018) <http://meity.gov.in/content/information-technology-act-2000>

Ministry of Justice:

‘Criminal Justice System statistics quarterly: December 2017’ (*Gov.uk*, 17 May 2018) <https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2017>

‘Malicious Communications Impact Statement’ (*Gov.uk*, 30 May 2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/321285/malicious-communicationss-impact-assessment.pdf>

Ministry of Justice and Lord Faulks QC, ‘Lord Faulks QC speech to the Criminal Justice Management Conference’ (*Gov.uk*, 25 September 2014) <https://www.gov.uk/government/speeches/lord-faulks-qc-speech-to-the-criminal-justice-management-conference>

Myres C B, ‘5 years ago today Twitter launched to the public’ (*TNW*, 15 July 2015) <https://thenextweb.com/twitter/2011/07/15/5-years-ago-today-twitter-launched-to-the-public/>

Myers F, ‘We must have the right to insult politicians’ (*Spiked*, 25 September 2018) <https://www.spiked-online.com/2018/09/25/we-must-have-the-right-to-insult-politicians/>

National Crime Agency:

‘National Cyber Crime Unit’ (*NCA*, 2018) <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit>

‘Organised Crime Groups’ *(NCA*, 2017) <http://www.nationalcrimeagency.gov.uk/crime-threats/organised-crime-groups>

NSPCC, ‘Online abuse: What is online abuse?’ (*NSPCC*, 2018) <https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/>

Ofcom:

‘About Ofcom’ (*Ofcom*, 2019) <https://www.Ofcom.org.uk/aboutOfcom>

‘Phones, telecoms and internet’ (*Ofcom*, 2019) <https://www.Ofcom.org.uk/phones-telecoms-and-internet>

‘News consumption in the UK: 2016’ (*Ofcom*, 29 June 2017) 34 <https://www.ofcom.org.uk/__data/assets/pdf_file/0016/103570/news-consumption-uk-2016.pdf>

‘The UK is now a smartphone society’ (*Ofcom*, 6 August 2015) <https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2015/cmr-uk-2015>

Office of National Statistics:

‘Internet users, UK: 2018’ (*Office of National Statistics*, 31 May 2018) <https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2018>

‘Internet access – households and individuals, Great Britain: 2017’ (*Office of National Statistics*, 3 August 2017) <https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2017>

Office of Legislative Drafting and Publishing, 'Guidelines for the Classification of Publications 2005: as amended' (*Gov.au*, 19 March 2008) <https://www.legislation.gov.au/Details/.../1ac3d219-38d6-4987-b21f-9e4b6ee27302>

Office of the eSafety Commissioner:

'eSafety Commissioner (*Australian Government*, 2019) <https://www.esafety.gov.au/>

'eSafetyWomen' (*Australian Government*, 2018) <https://www.esafety.gov.au/women/about-us>

'Role of the Office' (*Australian Government*, 2018) <https://www.esafety.gov.au/about-the-office/role-of-the-office>

Omand D, 'The dark net: Policing the internets underworld' (2016) Winter 2015/16 World Policy Journal <https://worldpolicy.org/2015/12/09/the-dark-net-policing-the-internets-underworld/>

Padte R K, 'Keeping women safe? Gender, online harassment and Indian law' (*Internet Democracy Project*, 29 June 2013) <https://internetdemocracy.in/reports/keeping-women-safe-gender-online-harassment-and-indian-law/>

Parliament of Australia, 'Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019' (*Parliament of Australia*, 2019) <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1201>

Penning M, 'Computer Misuse Act 1990: Written question – 222192' (*Parliament.uk*, 22 January 2015) <http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2015-01-27/222192/>

Personal, Social, Health and Economic Association, 'Parents call for education to address sexting by children and young people' (*PSHE Association*, 20 July 2016) <https://www.pshe-association.org.uk/news/parents-call-education-address-sexting-children>

Powell-Jones H, 'Online Social Media: Law and Ethics' (*Online Media Law UK*, 2019) <https://cml.sad.ukrd.com/document/612785.pdf>

Rosen G, 'Facebook Publishes Enforcement Numbers for the First Time' (*Facebook*, 15 May 2018) <https://newsroom.fb.com/news/2018/05/enforcement-numbers/>

Samaritans, 'Samaritans Rader' (*Samaritans*, 10 March 2015) <https://www.samaritans.org/how-we-can-help-you/supporting-someone-online/samaritans-radar>

Saunders A, 'Facebook Hacker committed serious offence' (*CPS: News Brief*, 17 February 2017) <http://blog.cps.gov.uk/2012/02/facebook-hacker-committed-serious-offence.html>

Senator the Hon Mitch Fifield, 'Esafety Commissioner to enhance online safety for all Australians' (*Senator the Hon Mitch Fifield*, 20 June 2017)

<http://mitchfifield.com/Media/MediaReleases/tabid/70/articleType/ArticleView/articleId/1380/eSafety-Commissioner-to-enhance-online-safety-for-all-Australians.aspx>

Spiegel J, 'Germany's Network Enforcement Act and its impact on social networks' (*TaylorWessing*, 2018) <https://www.taylorwessing.com/download/article-germany-nfa-impact-social.html>

Statista, 'Number of internet users worldwide from 2005 to 2017 (in millions)' (*Statista*, 2018) <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/>

Techopedia, 'Artificial Intelligence (AI)' (*Techopedia*, 2019) <https://www.techopedia.com/definition/190/artificial-intelligence-ai>

The Crown Prosecution Service:

'Extreme Pornography' (*CPS.gov*, 2019) <https://www.cps.gov.uk/legal-guidance/extreme-pornography>

'The Crown Prosecution Service' (CPS.gov, 2019) <https://www.cps.gov.uk/>

'Computer Misuse Act 1990' (*CPS.gov*, 2018) <https://www.cps.gov.uk/legal-guidance/computer-misuse-act-1990>

'Cybercrime - Legal Guidance' (*CPS.gov*, 2018) <https://www.cps.gov.uk/legal-guidance/cybercrime-legal-guidance>

'Guidelines on Prosecuting Cases Involving Communications Sent Via Social Media' (*CPS.gov*, 2018) < https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media

'Hate crime' (*CPS.gov*, 2018) <https://www.cps.gov.uk/hate-crime>

'Revenge Pornography - Guidelines on prosecuting the offence of disclosing private sexual photographs and films' (*CPS.gov*, 2018) <http://www.cps.gov.uk/legal/p_to_r/revenge_pornography/>

'The Code for Crown Prosecutors' (*CPS.gov*, 26 October 2018) <https://www.cps.gov.uk/publication/code-crown-prosecutors>

'Inchoate offences' (*CPS.gov*, 2017) <http://www.cps.gov.uk/legal/h_to_k/inchoate_offences/>

'Racist and Religious Hate Crime - Prosecution Guidance' (*CPS.gov*, 2017) <http://www.cps.gov.uk/legal/p_to_r/racist_and_religious_crime/#a07>

'Stalking and Harassment' (*CPS.gov*, 2017) <http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/>

'The Criminal Justice System' (CPS.gov, 2017) <https://www.cps.gov.uk/criminal-justice-system>

'Violent Extremism and Related Criminal Offences' (*CPS.gov*, 2017) <https://www.cps.gov.uk/publications/prosecution/cases_of_inciting_racial_and_religious_hatred_and_hatred_based_upon_sexual_orientation.html>

'Guidelines on Prosecuting Cases Involving Communications Sent Via Social Media' (*CPS.gov*, 2016)

<http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/>

'Man sentenced for "Revenge Porn" – Reading' (*CPS.gov*, 2015) <http://www.cps.gov.uk/thames_chiltern/cps_thames_and_chiltern_news/man_sentenced_for__revenge_porn____reading/>

'Guidelines on Prosecuting Cases Involving Communications Sent via Social Media' (*CPS.gov*, 2013) <http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/index.html>

The Crown Prosecution News Brief, 'DPP Statement on Tom Daley Case and Social Media Prosecutions' (*CPS.gov,* 2012) <http://blog.cps.gov.uk/2012/09/dpp-statement-on-tom-daley-case-and-socialmedia-prosecutions.html>

The Fawcett Society, 'Twitter is "failing women" experiencing online threats and harassment' (*The Fawcett Society*, 22 August 2017) <https://www.fawcettsociety.org.uk/news/twitter-failing-women-experiencing-online-threats-harassment>

The Guardian, 'Facebook Files' (*The Guardian*, 2019) <https://www.theguardian.com/news/series/facebook-files>

The International Forum for Responsible Media Blog:

Woods L, 'When is Facebook liable for illegal content under the E-commerce Directive? CG v. Facebook in the Northern Ireland courts'(*The International Forum for Responsible Media Blog*, 28 January 2017) <https://inforrm.org/2017/01/28/when-is-facebook-liable-for-illegal-content-under-the-e-commerce-directive-cg-v-facebook-in-the-northern-ireland-courts-lorna-woods/>

Alex Bailin QC & Edward Craven, 'Prosecuting social media: the DPP's interim guidelines' (*The International Forum for Responsible Media Blog*, 23 December 2012) <https://inforrm.wordpress.com/2012/12/23/prosecutingsocial-media-the-dpps-interim-guidelines-alex-bailin-qc-and-edward-craven/>

De Wilde G, 'News: "Twitter Joke" Case goes to the High Court' (*The International Forum for Responsible Media Blog,* 8 February 2012) <https://inforrm.org/2012/02/08/news-twitter-joke-case-goes-to-the-high-court-gervase-de-wilde/>

Thinkuknow, 'What we see, say, do online' (*Thinkuknow.org.au*, 2018) <https://www.thinkuknow.org.au/what-we-see-say-do-online>

Twitter:

'About intimate media on Twitter' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/intimate-media>

'Abusive behavior' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/abusive-behavior>

'Guidelines for law enforcement' (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support>

‘Hateful conduct policy’ (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy>

‘How to use advanced muting options’ (*Twitter*, 2019) <https://help.twitter.com/en/using-twitter/advanced-twitter-mute-options>

‘Legal request FAQs’ (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/twitter-legal-faqs>

‘Our approach to policy development and enforcement philosophy’ (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/enforcement-philosophy>

‘Our range of enforcement options’ (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/enforcement-options>

‘Violent threats and glorification of violence’ (*Twitter*, 2019) <https://help.twitter.com/en/rules-and-policies/violent-threats-glorification>

‘Transparency Report: Information Requests’ (*Twitter*, 2018) <https://transparency.twitter.com/en/information-requests.html>

‘Twitter Rules Enforcement’ (*Twitter*, 2018) <https://transparency.twitter.com/en/twitter-rules-enforcement.html#twitter-rules-enforcement-jan-jun-2018> accessed 18 February 2019

Young Minds, ‘Resilience for the digital world’ (*Young Minds*, January 2016) <https://youngminds.org.uk/assets/0002/6859/Resilience_for_the_Digital_World_YM_Positioning.pdf>

Zuckerberg M, ‘Building Global Community’ (*Facebook*, 16 February 2017) <https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/>

Media

BBC Panorama, ‘What Facebook Knows About You’ (*BBC IPlayer*, 8 May 2017) <https://www.bbc.co.uk/iplayer/episode/b08qgbc3/panorama-what-facebook-knows-about-you>

Guardian News, ‘Mark Zuckerberg testifies before Congress’ (*YouTube,* 10 April 2018) <https://www.youtube.com/watch?v=mZaec_mlq9M>

PBS NewsHour, ‘Facebook CEO Mark Zuckerberg testifies before the European Union Parliament’ (*YouTube*, 22 May 2018) <https://www.youtube.com/watch?v=Y70LrlzrkNk>

Appendix A: Social Media Bill

A Bill to make provision for protecting persons from abusive conduct aided by new technology in particular, social media.

(1) Cyber Harassment

(1) A person is guilty of an offence if:
- (a) The person uses technology in a way which the reasonable person would consider as amounting to causing distress or anxiety to another; and
- (b) The defendant knows or ought to know that their behaviour may cause another distress or anxiety

(2) Interpretation:
- (a) 'Technology' is defined as a device for storing, processing and retrieving information
- (b) 'Anxiety' is defined as something just short of a recognised psychiatric illness
- (c) 'Distress' is defined as oppressive and unreasonable behaviour

(2) Cyberstalking

(1) A person is guilty of an offence if:
- (a) The person uses technology in a way which the reasonable person would consider as amounting to causing distress or anxiety to another; and
- (b) The behaviour can be considered as continued unwanted contact; and
- (c) The defendant knows or ought to know that their behaviour may cause another distress or anxiety

(2) Interpretation:
- (a) 'Technology' is defined as a device for storing, processing and retrieving information
- (b) 'Anxiety' is defined as something just short of a recognised psychiatric illness
- (c) 'Distress' is defined as oppressive and unreasonable behaviour

(3) Cyber Related Revenge Pornography

(1) A person commits an offence if:
- (a) He intentionally or recklessly discloses a private sexual photograph or film to another; and

(b) Knowingly discloses a private sexual photograph or film without the consent of the individual who appears in the content; and
(c) The disclosure is made using technology

(2) Where an allegation has been made that an offence to which this clause applies has been committed against a person, no matter relating to that person shall during that person's lifetime be included in any publication

(3) Interpretation:
(a) 'Sexual' is defined as a person:
a. Engaged in sexual intercourse; or
b. Unclothed external genitalia, the perineum and anus of a male or female; Buttocks of a male or female; Breasts and nipples of a female; and covered erectile genitalia of a male are clearly visible; or
c. A photo or film that the reasonable person would consider as sexually explicit
(b) 'Photo or film' is defined as a still or moving picture, including a photoshopped image or video
(c) A person "discloses" something to a person if, by any means, he or she gives or shows it to the person or makes it available to the person
(d) 'Technology' is defined as a device for storing, processing and retrieving information

(4) Online Abuse

(1) An offence is committed if:
a. A person uses technology in a way which the reasonable person would consider as amounting to causing distress or anxiety to send;
i. Content that can be labelled as grossly offensive or menacing by reasonable members of society; and
ii. The defendant knows or ought to know that their behaviour may cause another distress or anxiety

(2) An offence is committed if;
a. A person uses technology in a way which the reasonable person would consider as amounting to causing distress or anxiety to send;
b. Content that is either:
i. False information which D knows to be false; or
ii. Is produced using false credentials; and

c. The conduct can be labelled as grossly offensive or menacing by reasonable members of society; and
d. The defendant knows or ought to know that their behaviour may cause another distress or anxiety

(3) In matters relating to obscene material, the Obscene Publications Act 1949 and 1964 will be utilised

(4) An offence is committed if;
a. A person uses technology in a way which the reasonable person would consider as amounting to causing distress or anxiety to send;
i. Explicit threats of rape or sexual violence; or
ii. Credible threats of violence; and
b. The defendant knows or ought to know that their behaviour may cause another distress or anxiety

(5) Interpretation:
a. 'Technology' is defined as a device for storing, processing and retrieving information
b. 'Grossly Offensive' is defined as more than;
i. Offensive, shocking or disturbing; or
ii. Satirical, iconoclastic or rude comment; or
iii. The expression of unpopular or unfashionable opinion about serious or trivial matters, or banter or humour, even if distasteful to some or painful to those subjected to it; or
iv. An uninhibited and ill thought out contribution to a casual conversation where participants expect a certain amount of repartee
c. 'Menacing' is defined as something just short of a credible threat
d. 'False credentials' include fake accounts
e. 'Anxiety' is defined as something just short of a recognised psychiatric illness
f. 'Distress' is defined as oppressive and unreasonable behaviour
g. 'Explicit' is defined as a clear and precise threat of sexual violence

(5) Inciting Others

(1) It is an offence to intentionally incite multiple persons to target another in a way which D reasonably believes will cause harassment of

another

(2) It is an offence to intentionally incite others to commit a further criminal offence either governed by statute or the common law which D reasonably believes will result in a further criminal offence taking place

(3) Interpretation:
   a. 'Harassment' consists of:
      i. The use of technology which;
      ii. The reasonable person would consider amounts to distress or anxiety
   b. 'Technology' is defined as a device for storing, processing and retrieving information
   c. 'Anxiety' is defined as something just short of a recognised psychiatric illness
   d. 'Distress' is defined as oppressive and unreasonable behaviour
   e. 'Belief' is defined as something short of knowledge
   f. 'Multiple' is defined as two or more people

(6) Online Hate

(1) If any of the behaviours listed in this Bill are targeted at a person:
   a. Because of a protected characteristic or presumed characteristic; and
   b. There is an intention on part of D to target another because of a protected characteristic, this will be considered as a hate crime.

(2) Interpretation
   a. Protected characteristics covers the following:
      i. Race;
      ii. Ethnicity;
      iii. National Origin;
      iv. Religious Affiliation;
      v. Sexual Orientation;
      vi. Caste;
      vii. Sex;
      viii. Gender or Gender Identity; or
      ix. Disability

(7) Computer Misuse

(1) In matters relating to Computer Misuse, the Computer Misuse Act 1990 will be utilised

(8) e-Safety Commissioner

(1) The Secretary of State must create an e-Safety Commissioner

(2) The e-Safety Commissioner will oversee the creation of a universal code of conduct with the aid of stakeholders, not-for-profit organisations, a Digital Authority and any other body the e-Safety Commissioner feels has appropriate knowledge to aid discussions:
   a. The e-Safety Commissioner will make the final decision on the content of the universal code of conduct
   b. The universal code of conduct will implement a voluntary levy to be paid by all social media companies
      i. The e-Safety Commissioner will determine the levy to be paid; and
      ii. The levy will not exceed the percentage levy paid under the Gambling Act 2005
   c. Failure of social media companies to comply with the universal code of conduct will result in a fine

(3) The e-Safety Commissioner will create a Digital Authority to oversee the day-to-day running of the universal code of conduct
   a. The Digital Authority must:
      i. Regulate and enforce the universal code of conduct;
      ii. Act as an advisory body to the Crown Prosecution Service; and
      iii. Investigate complaints by online users against social media companies

(4) The e-Safety Commissioner and the Digital Authority will also:
   a. Oversee the implementation of Digital Literacy educational schemes across schools throughout the United Kingdom;
   b. Ensure parents, teachers and the police receive adequate education relating to conduct carried out *via* social media; and
   c. Aid research into social media

(5) Interpretation:
   a. ‘Stakeholders’ will include social media companies

‘Social media companies’ are defined as website hosts who, for profit-making purposes, operate an Internet platform which enables users to create content and communicate instantly. Journalistic websites and websites with less than 10,000 global users are exempt.

Appendix B: Draft Universal Code of Conduct

This code provides a universally accepted standard which all 'social media companies must adhere to. For the purpose of this code of conduct 'social media companies' are defined as 'website hosts who, for profit-making purposes, operate an Internet platform which enables users to create content and communicate instantly. Journalistic websites and websites with less than 10,000 global users,[1] are exempt from the conditions listed below.'

General Conditions

1. Social media companies must ensure maximum privacy settings are listed as the default option when a person creates a social media profile.
2. Maximum privacy settings are compulsory for all those aged under 18.
3. Social media companies must remove unlawful content within 48 hours of being made aware of the content.
4. Terrorist content and hate related speech must be removed within 24 hours:
    a. Hate speech is defined as content that targets someone's 'race, ethnicity, national origin, religious affiliation, sexual orientation, caste, sex, gender, gender identity and serious disease or disability.'[2]
5. Terms of service agreements must be written in clear English and where appropriate, examples are given.
6. Users must be able to report objectionable content with ease, and where appropriate social media companies must classify reported content. For instance, content that incites violence, hate related speech and sexual exploitation.
7. Where a data breach has occurred, social media companies must make the e-Safety Commissioner aware of the breach within 48 hours of the breach coming to the company's attention.
8. Social media companies must continue to invest in AI technology to flag inappropriate content **BEFORE** it becomes publicly viewable.
9. Mandatory training for all social media moderators:
    a. All moderators will be issued with training manuals which clearly illustrates content which is and is not acceptable on a given site;
    b. All manuals must be in clear English;
    c. Where moderators believe that a person or persons are at risk, reporting mechanisms are in place to flag content to appropriate authorities; and
    d. Moderators must receive updated training every 18 months.

[1] This ensures that small companies are not at an unfair advantage and free competition is protected, whilst giving protection to freedom of speech

[2] Facebook, 'Community Standards: Hate Speech' (*Facebook*, 2018) <https://www.facebook.com/communitystandards/hate_speech> accessed 9 December 2018

10. Links must be available for online users to seek further support for a range of issues, including, self-harm, suicide, mental health awareness, bullying and victim support.

Unacceptable Content

1. Hate speech:
    a. Hate speech is defined as content that targets someone's 'race, ethnicity, national origin, religious affiliation, sexual orientation, caste, sex, gender, gender identity and serious disease or disability.'[3]
2. Revenge Pornography:
    a. Revenge pornography is defined as sexually explicit or nude images of another, or images of a sexual nature which have been uploaded without the consent of the person capsulated in the image:
        i. Image includes both still and moving pictures.
        ii. Sexual' is defined as a person:
            1. Engaged in sexual intercourse; or
            2. Unclothed external genitalia, the perineum and anus of a male or female; Buttocks of a male or female; Breasts and nipples of a female; and covered erectile genitalia of a male are clearly visible; or
            3. A photo or film that the reasonable person would consider as sexually explicit
3. Directly abusive content which amounts to the trolling or bullying of another.
4. Dogpiling:
    a. Encouraging other Internet users to target a specific individual.
5. Threats of violence or threats of a sexual nature:
    a. This includes physical threats of violence, threats of rape and threats of sexual assault.

Social Media Levy

1. All social media companies will be asked to pay a voluntary levy to aid research, education and the Digital Authority in helping to tackle online abuse.
2. The levy will be decided by the e-Safety Commissioner, but it will not exceed the Gambling Act levy.
3. All earnings gained from the social media levy will be used for:
    a. Universal educational schemes relating to Digital Literacy skills as overseen by the e-Safety Commissioner. These

[3] Facebook, 'Community Standards: Hate Speech' (*Facebook*, 2018) <https://www.facebook.com/communitystandards/hate_speech> accessed 9 December 2018

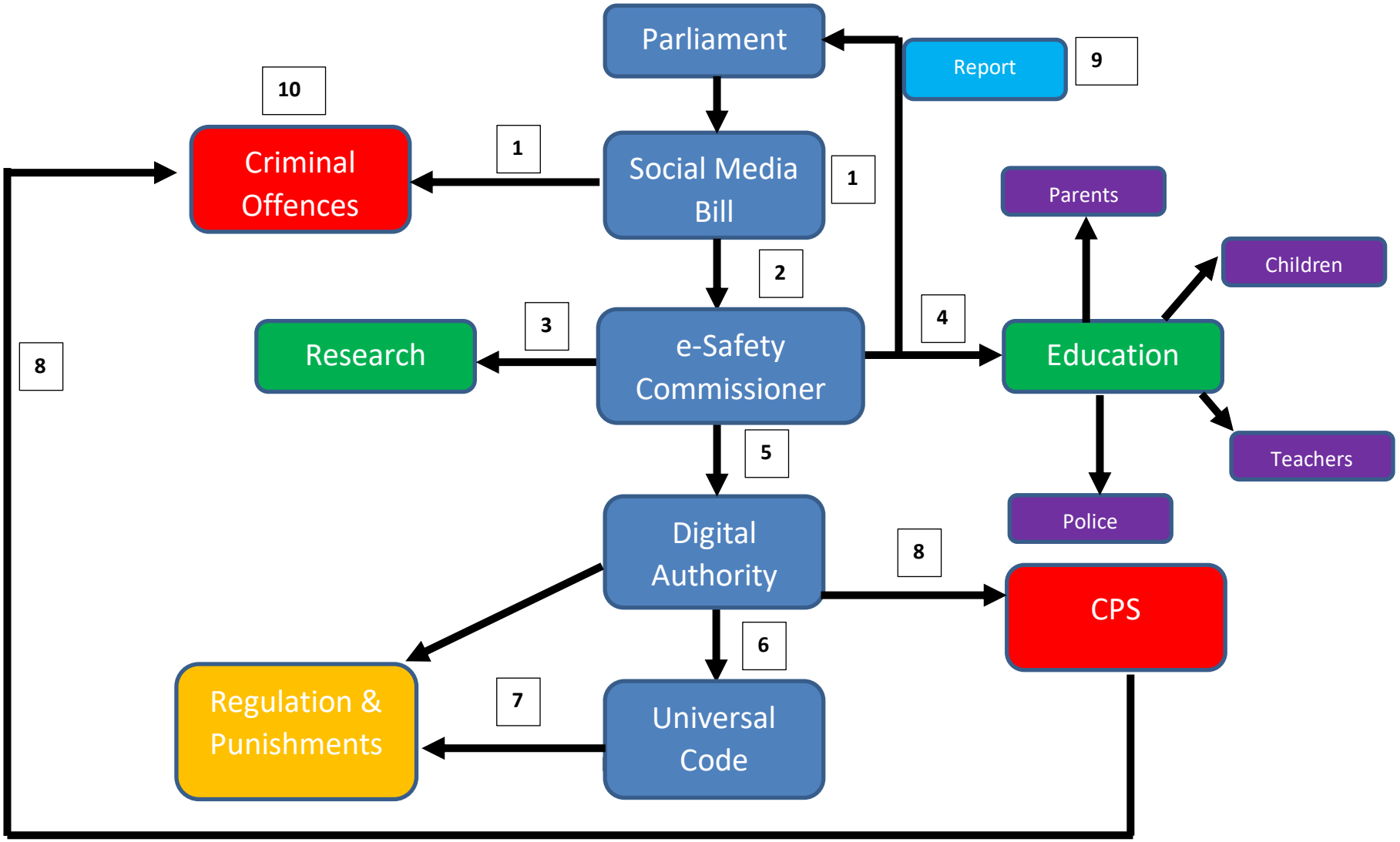
programmes will be aimed at school aged children, parents, the criminal justice system and teachers;
b. Help with the financial costs of creating a Digital Authority; and
c. Aid continued research into social media behaviour.

Digital Authority and Fines

1. To oversee the implementation of the universal code of conduct, regulate social media companies and act as an advisor to the CPS, the e-Safety Commissioner will create a Digital Authority:
    a. The Digital Authority will deal with the day-to-day regulation of social media companies.
2. The Digital Authority may issue fines to social media companies who are in clear breach of the universal code of conduct.
3. Social media companies may appeal to the e-Safety Commissioner in relation to any fines issued, or decisions made by the Digital Authority.
4. Social media companies may seek Judicial review if they believe that a decision made by the e-Safety Commissioner is unlawful.

All social media companies must adhere to the terms above. Where there is a conflict between social media companies terms of service agreements and the universal code of conduct, the universal code will prevail.

Appendix C: Recommendations Flowchart



Appendix D: Flow chart explanation

Point 1

A Bill to make provision for protecting persons from abusive conduct aided by Social Media. The Bill itself will have two main purposes. First, it will criminalise abusive conduct aimed at individuals *via* social media, as illustrated in Appendix A. Second, it will provide the legal authority for an e-Safety Commissioner and Digital Authority to be created.

Point 2

The e-Safety Commissioner, alongside the Digital Authority, will oversee the regulation of social media companies through the creation of a universal code of conduct (see point 6); oversee the implementation of compulsory educational schemes across the United Kingdom, aimed at parents, children, teachers and the criminal justice system, alongside funding research projects examining online behaviours. The e-Safety Commissioner will also investigate any complaints against the Digital Authority in a clear and transparent manner to ensure the protection of freedom of expression.

Point 3

Research is an important aspect of understanding online behaviour. The e-Safety Commissioner will oversee and fund research in this area, with the aid of the social media levy. Research will include, but is not limited to, online safety, social media conduct, privacy, online behaviours and educational schemes set up by the e-Safety Commissioner and not-for-profit organisations.

Point 4

Education is an important aspect in tackling online abuse. As outlined in the recommendations chapter, social media-based education needs to be a compulsory subject within all educational institutions. The e-Safety Commissioner will oversee the running of educational programmes aimed at advancing Digital Literacy skills in children. In addition, educational schemes will be generated targeting teachers, parents and the criminal justice system. These educational programmes will be funded by the social media levy.

Point 5

The main role of the Digital Authority will be to ensure that social media companies are adhering to the universal code of conduct. The Digital Authority will answer to the e-Safety Commissioner. The Digital Authority can also impose fines on social media companies who fail to comply with the universal code of conduct. These fines, alongside the social media levy, will be used to fund research into social media usage and behaviour, help with

the costs of implementing an educational scheme and help towards the costs of social media regulation.

Point 6

The e-Safety Commissioner, the Digital Authority and stakeholders will also be responsible for the creation and implementation of a universal code of conduct. As outlined in the recommendations chapter, the universal code of conduct will consist of a universal set of standards which all social media companies must adhere to. An example of the universal code of conduct can be found in Appendix B. However, the day-to-day moderation of this code of conduct will be overseen by the Digital Authority.

Point 7

The Digital Authority will investigate complaints from online users concerning decisions made by social media companies and regulate the implementation of the universal code of conduct. They will work alongside the e-Safety Commissioner to run educational campaigns, oversee the day-to-day regulation of social media companies and aid future research into online behaviours.

Point 8

Where the Digital Authority feels that a criminal offence has taken place, as governed under the Social Media Bill or another Act of Parliament, they will refer the case to the Crown Prosecution Service (CPS), who will decide if any further action should be taken. They will also act as an advisory body for the CPS.

Point 9

On a yearly occurrence, the e-Safety Commissioner will report either to Parliament or the Communications Committee to answer questions relating to the regulation of social media companies. The e-Safety Commissioner will also produce a yearly report detailing key decisions made, failures in the system and recommendations for the year ahead.

Point 10

See Appendix A.