Law Commission
Reforming the law

Abusive and Offensive Online Communications: A Scoping Report

HC 1682

Law Com No 381

Law Commission
Reforming the law

(Law Com No 381)

Abusive and Offensive Online Communications: A Scoping Report

Presented to Parliament pursuant to section 3(2) of the Law Commissions Act 1965

Ordered by the House of Commons to be printed on 1 November 2018

HC 1682

This publication is available at www.gov.uk/government/publications.

ISBN 978-1-5286-0848-0

CCS Ref = CCS1018845550

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

The Law Commission

The Law Commission was set up by the Law Commissions Act 1965 for the purpose of promoting the reform of the law.

The Law Commissioners are:

The Right Honourable Lord Justice Green, Chairman

Professor Nick Hopkins

Stephen Lewis

Professor David Ormerod QC

Nicholas Paines QC

The Chief Executive of the Law Commission is Phil Golding.

The Law Commission is located at 1st Floor, Tower, 52 Queen Anne's Gate, London SW1H 9AG.

The terms of this report were agreed on 25 October 2018.

The text of this report is available on the Law Commission's website at http://www.lawcom.gov.uk.

Contents

Glossary

This is not an exhaustive comprehensive glossary of terms relating to the internet or communications online. It defines only the terms related to online communication that are used in this Scoping Report.

App

Short for “application”, this is software that can be installed on a mobile device, such as a tablet or mobile phone, or a desktop computer.

Blog

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. To “blog” something is also a verb, meaning to add content to a blog, and a person responsible for writing blog entries is called a “blogger”. Microblogging refers to blogging where the content is typically restricted in file size; microbloggers share short messages such as sentences, video links or other forms of content. Twitter is an example of a microblog.

Catfishing

Luring someone into a relationship by adopting a fictional online persona.

Chatroom

A feature of a website where individuals can come together to communicate with one another. Chatrooms can often be dedicated to users with an interest in a particular topic. Chatrooms can have restricted access or be open to all.

Comment

A response to another person’s message – such as a **blog** post, or **tweet** – often over a social media platform.

Crowdfunding

The practice of funding a project or venture, or raising money for a charity, by collecting money from a large number of people who each contribute a sum, typically via the internet. Websites have been created specifically for crowdfunding, such as www.justgiving.com or www.kickstarter.com.

Cyberbullying

The use of the internet enabled forms of communication to bully a person, typically by sending messages of an intimidating or threatening nature.

Cyberstalking

A form of stalking that takes place over the internet.

Deepweb and Darkweb

The Deepweb refers to any parts of the World Wide Web that cannot be found using conventional search engines like Google. This could be because the content is restricted by the website creators. The Darkweb refers to the small portion of the Deepweb that can only be accessed through the use of specific software, such as the TOR browser. It has both legitimate and illegitimate uses, and is commonly used for facilitating the distribution of controlled drugs and indecent photographs of people aged under 18 years.

Deepfake pornography

A blend of the words “deep learning” and “fake”, “deepfake” pornography involves combining the face or head of one person, with the torso and limbs of another (often performing sexual acts). It is achieved through the use of an artificial intelligence-based human image synthesis technique.

Downblousing

The act of taking a photograph or video down a woman or girl’s shirt or dress without her consent.

Doxing

Searching for and publishing private or identifying information about a particular individual on the web, typically with malicious intent.

Email bombing service

A service that sends very large volumes of emails to a specific email address, aiming to overflow it and crash the host mail server.

Facebook

A social media platform which connects users from all over the world and enables them to post, share, and engage with a variety of content such as photos and status updates.

Facebook messenger

A private messaging service provided by Facebook, whereby a Facebook user can contact one or more of their Facebook **friends** either in one-to-one or group communication. Messages sent will only be visible to those involved in the messages or group chats.

Fake news

False, often sensational, information disseminated under the guise of news reporting.

Friend

The term used on social media services such as **Facebook** to refer to an individual who is added to a user's social network on the platform. A person may allow this "friend" to view their profile, or particular parts of it (for example, certain posts or messages). It is also used as a verb, for example, to "friend" a person, means to add them to your social network. Facebook "friends" may not actually be "friends" in the conventional understanding of the term. Someone could "friend" a complete stranger.

Follow

"Following" another user of certain social media platforms (for example, **Twitter** or **Instagram**) means that you will receive updates from that user, which will appear in your **newsfeed**.

Handle

The term used to describe someone's username on **Twitter**. For example, the Law Commission's Twitter handle is @Law_Commission.

Hashtag

A hashtag is a **tag** usually used on social networks such as **Twitter** or **Facebook**. Social networks use hashtags to categorise information and make it easily searchable for users. It is presented as a word or phrase preceded by a "". For example, a current well-known hashtag is MeToo.

Image hashing

Image hashing refers to the process of examining the contents of an image, and constructing a digital hash value that uniquely identifies an input image based on the contents of an image. The hash value can then be used to search for other instances of the image.

Instagram

A photo sharing **app** that allows users to take photos, apply filters to their images, and share the photos instantly on the Instagram network and other social networks such as **Facebook** or **Twitter.**

Instant messaging (IM)

A form of real-time, direct text-based communication between two or more people. More advanced instant messaging software also allows enhanced modes of communication, such as live voice or video calling.

Internet Access Provider

A company that provides subscribers with access to the internet.

Internet Service Provider

A broader term than Internet Access Provider referring to anything from a hosting provider to an app creator.

IP address

An “internet protocol” address is a numerical label which identifies each device on the internet, including personal computers, tablets and smartphones.

Liking

Showing approval of a message posted on social media by another user, such as his or her **Facebook** post, by clicking on a particular icon.

Live streaming

The act of delivering video content over the internet in real-time. This term was popularised in social media by **apps** such as **Periscope**.

Meme

A thought, idea, joke or concept that has been widely shared online, often humorous in nature; typically an image with text above and below it, but sometimes in video and link form.

Offline communication

Communication that does not use the internet (for example, having a face-to-face conversation or sending a letter).

Online communication

Communication via the internet between individuals and/or computers with other individuals and/or computers.

Periscope

A social video **app** that allows users to broadcast live video from wherever they are and to engage with others’ videos, browse live or recent broadcasts, and follows users to receive notifications.

Post or posting (on social media)

A comment, image or video that is sent so as to be visible on a user’s social media page or **timeline** (whether the poster’s own or another’s).

Private message

A private communication between two people on a given platform which is not visible or accessible to others.

Profile page

A display of personal information and posts associated with a person on a social media service.

Replying

An action on, for example, **Twitter** that allows a user to respond to a tweet through a separate tweet that begins with the other user's @username.

Retweeting

The re-sharing (forwarding) on **Twitter** by a person (B) of a message received from another person (A), using the re-tweet button and attributing the message to A.

Sharing

The broadcasting by users of **social media** of web content on a social network to their own social media page, or to the page of a third party.

Skype

A free program that allows for text, audio and video chats between users; it also allows users to place phone calls through their Skype account.

SnapChat

A social **app** that allows users to send and receive time-sensitive photos and videos known as "snaps" to other users chosen by them. Once the snap is opened by the receiver, there is a time limit before the snap is closed and cannot be opened again (typically 10 seconds). Users can add text and drawings to their snaps and control the list of recipients to whom they send them.

Social media

Websites and apps that enable users to create and share content or to participate in social networking.

Social media platform

Refers to the underlying technology which facilitates the creation of social media websites and applications. From a user's perspective, it enables blogging and microblogging (such as **Twitter**), photo and video sharing (such as **Instagram** and **YouTube**), and the ability to maintain social networks of friends and contacts. Some platforms enable all of these in one service (through a website and/or an application for a desktop computer or mobile phone) as well as the ability for third-party applications to integrate with the service.

Social Networking Service

A service provided by an internet company which facilitates the building of social networks or social relations with other people, through the sharing of information. Each service may differ

and target different uses and users. For example, facilitating connections between business contacts only, or only particular types of content, such as photos.

Tag

A **social media** function used commonly on **Facebook**, **Instagram** and **Twitter**, which places a link in a posted photograph or message to the profile of the person shown in the picture or targeted by the update. The person that is "tagged" will receive an update that this has occurred.

Tinder

A location-based social (online dating) search mobile **app** that allows users to like (swipe right) or dislike (swipe left) other users, and allows users to chat if both parties swiped to the right (a match).

Troll

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.

Tweet

A post on the social networking service "**Twitter**". Tweets can contain plain text messages (not more than 280 characters in the English version of the service), or images, videos, or polls. Users can tweet to another person (@mention tweets) so as to ensure they will be notified of the tweet, or can also message them directly. Other users can retweet the tweets of others amongst their connections on the platform.

Twitter

A social network that allows users to send "**tweets**" to their followers and/or the public at large.

Upskirting

The act of taking a photograph or video underneath a woman's skirt (or a man's kilt) without consent, typically in a public place.

Viral

The phenomenon whereby a piece of content, such as a video, photo, blog article or social media post, is sent and shared frequently online, resulting in it being seen widely across many web users.

Vlogging

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").

Webcam

A video camera connected to a computer, which can be used through a variety of different social media services for video calls between users or video conferencing.

WhatsApp

An encrypted instant messaging service for one-to-one or group chat on mobile devices.

YouTube

A video-sharing website that allows registered users to upload and share videos, and for any users to watch videos posted by others.

Webchat

Communicating either one-to-one or in a group over the internet, usually through a text-based application such as **WhatsApp** or **Facebook** private messenger.

List of statute abbreviations

Below is a list of the abbreviations used throughout the Scoping Report for the most commonly cited statutes.

CA 2003: Communications Act 2003

CAA 1981: Criminal Attempts Act 1981

CDA 1998: Crime and Disorder Act 1998

CJA 2003: Criminal Justice Act 2003

CJCA 2015: Criminal Justice and Courts Act 2015

CJIA 2008: Criminal Justice and Immigration Act 2008

DPA 2018: Data Protection Act 2018

IDCA 1981: Indecent Displays (Control) Act 1981

MCA 1988: Malicious Communications Act 1988

OPA 1959: Obscene Publications Act 1959

PHA 1997: Protection from Harassment Act 1997

POA 1986: Public Order Act 1986

SCA 2007: Serious Crime Act 2007

SOA 2003: Sexual Offences Act 2003

Chapter 1: Introduction

1.1 In 2016 and 2017 the Law Commission held widespread consultations to ask which projects we should prioritise for review and possible future law reform. Offensive and abusive online communication was one of the most widely supported issues suggested, and a Law Commission review of the law in this area was specifically recommended by the All-Party Parliamentary Group on Domestic Violence in February 2017.[1] In February 2018, the Prime Minister announced that the Law Commission was to begin a six-month project to analyse the current criminal law relating to abusive and offensive online communication.[2]

1.2 The particular focus of this project was to establish whether abusive and offensive behaviour, which is illegal offline, is also illegal if engaged in wholly or partly online. In making that assessment, we undertook to look not only at the wording of the applicable statutes but also to:

(1) examine the terms of the offences that might apply to deal with behaviour in this context;

(2) to consider the way those offences have been interpreted in the courts; and

(3) to assess the way in which they are investigated and prosecuted.

1.3 The review is in two phases. This Scoping Report constitutes the first phase, setting out the current criminal law which applies to abusive and offensive online communication. Much of the relevant law predates the internet and this Scoping Report highlights some of the ways in which the exponential growth of online communication has created challenges for the applicable criminal law. The second phase of the project will look at possible recommendations for reform.[3]

1.4 In this Scoping Report we use "offline" as a way of referring to communication which does not take place via the internet. Offline communication would include, for example, face to face conversations and letters sent by post. The term "online" has been used in this Report to refer to any communication which takes place over the internet. This includes, for example, comments made in online games, via email, text message or social media, on blogs or over instant messaging services.

---

1 All-Party Parliamentary Group on Domestic Violence, *Tackling domestic abuse in a digital age* (February 2017) p 14, available at https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/04/APPGReport2017-270217.pdf. All website addresses referenced in this Scoping Report were last visited in October 2018.

2 The Rt Hon Theresa May MP, *Standards in Public Life* (6 February 2018), available at https://www.gov.uk/government/speeches/pm-speech-on-standards-in-public-life-6-february-2018.

3 The terms of reference for Phase 2 are yet to be agreed. More detail on the structure of this project can be found in HM Government, *Government response to the Internet Safety Strategy Green Paper* (May 2018) p 46, available at 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.

THE AGREED TERMS OF REFERENCE

1.5 The Terms of Reference require the Law Commission to draft a comprehensive paper:

(1) analysing the framework of offensive communications legislation as it applies to online communication; and

(2) setting out the impact of any deficiencies identified in the current legal framework, including whether the current law is effective in ensuring that what is illegal offline is also illegal online.

1.6 This review of the current law includes analysis of:

(1) the Malicious Communications Act 1988 ("MCA 1988"), particularly in relation to its effectiveness in dealing with communications involving many recipients or viewers;

(2) the overlap between section 127 of the Communications Act 2003 ("CA 2003") and the MCA 1988;

(3) the appropriateness of offences based on the words "grossly offensive" and whether they pose difficulties for the principle of legal certainty;

(4) the inconsistent requirements, across the current legislative provisions, to prove fault on the part of the person who sends the communication; and

(5) difficult concepts which may need to be reconsidered in the light of technological change. For example, who is "the sender" in the online context?

1.7 We have also considered, where relevant, how other jurisdictions have dealt with these issues.[4]

1.8 In addition, we have analysed overlap between laws applying to abusive and offensive online communication, and other areas of the criminal law.

1.9 Topics that are specifically stated to be outside our terms of reference are:

(1) terrorist offences committed online;

(2) child sexual exploitation; and

(3) the liability of internet platforms in relation to transmitting or storing abusive or offensive communications.

1.10 This is because Government already has separate active programmes of policy work underway in each of these areas.

---

[4] See paragraph 1.30.

THE SCOPE OF THIS REVIEW

1.11 In interpreting our terms of reference, we have taken a broad view of the concepts of "abusive" and "offensive" communication. Chapter 2 deals specifically with issues of definition surrounding offensiveness. "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. While many criminal offences could technically fall under these definitions, in this Scoping Report we are concerned with communication offences. It is in those offences where abuse of, and offence to, a person or people are the primary focus.

1.12 This construction of the terms of reference means that some offences that could be committed online are not addressed in this Scoping Report. For example, fraud, contrary to section 1 of the Fraud Act 2006, could in some cases be regarded as cruel, and consequently abusive; particularly if it results in a financial loss to the defrauded party. However, as the central focus of the fraud offence is the protection of rights and interests in property, we do not classify it as an abusive offence for the purposes of this analysis.

1.13 In line with the agreed Terms of Reference, this Scoping Report also does not include analysis of offences dealing specifically with child sexual abuse images and child exploitation online, terrorism offences, or the liability of internet service providers for transmitting or storing abusive or offensive communications. These were topics outside our terms of reference and are being addressed by Government as part of its wider Internet Safety Strategy.[5]

1.14 At the time of writing, the Attorney General's Office was preparing a response to its call for evidence on "The Impact of Social Media on the Administration of Justice".[6] We therefore have not considered issues concerning the impact of social media on the criminal trial process. Nor have we included any detailed analysis of contempt of court in this Report.

1.15 This Report considers how the criminal law deals with abusive and offensive communication generally. It has a particular focus on whether the recipient of online abusive and offensive communication has as much protection from the criminal law – both in theory and practice – as they would be afforded if the offending behaviour occurred offline.

---

5 See Department of Digital, Culture, Media and Sport, *Internet Safety Strategy – Green paper* (October 2017), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf, and HM Government, *Government response to the Internet Safety Strategy Green Paper* (May 2018), available at 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.

6 Attorney General's Office, *The Impact of Social Media on the Administration of Justice: A Call for Evidence* (September 2017), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/645032/Call_for_Evidence__Final_.pdf.

1.16 The Report is concerned only with the criminal law and its applicability and efficacy in this area. Any civil liability arising from online communications is not within the terms of reference for this analysis, although we mention it as context where relevant.

1.17 As we note further in Chapter 2, the right to freedom of expression in Article 10 of the European Convention on Human Rights is highly relevant to all online communications offences, and is considered – where particularly applicable – throughout this Report.

THE ROLE OF INTERNET PLATFORMS

1.18 As we have outlined above, the liability of internet platforms in relation to content that they transmit or store is explicitly outside the scope of this review.

1.19 It is undeniable that internet platforms have a crucial role to play in protecting users from the serious harms to which they can be exposed.[7] Major platforms such as Facebook and Instagram, Twitter, YouTube, Snapchat, Tumblr and others already take active steps to enforce acceptable user standards and shield users from harm. They do this through a combination of technological solutions,[8] user-based reporting,[9] and human review of content.[10]

1.20 Internet platforms also have an important role to play in police investigation of these offences. We look in detail at the ways in which service providers are frequently relied upon in the enforcement of abusive and offensive online communications offences, and some of the challenges which arise, in Chapter 2 of this paper.

1.21 In recent years, with the continued proliferation of harmful and abusive content, there have been prominent public calls for these platforms to do even more to protect the public, and suggestions that an enhanced regulatory regime may be necessary to enforce compliance.[11]

---

7 For further discussion, see A Nehaluddin, "Internet intermediary liability: a comparative overview" (2011) 17(4) *Computer Telecommunications Law Review* 108; L Scaife, "The interrelationship of platform providers and users in the regulation of Twitter and offensive speech – is there a right to be offensive and offended at content?" (2013) 18(4) *Communications Law* 128.

8 Such as the use of algorithms to identify and automatically remove illegal and/or inappropriate content. See Hate crime: abuse, hate and extremism online, Report of the Select Committee on Home Affairs (2017) HC 609 at [47] to [50], available at https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/60904.htm.

9 K Crawford and T Gillespie, "What is a flag for? Social media reporting tools and the vocabulary of complaint" (2016) 18(3) *New Media and Society* 410. For an example, see https://help.twitter.com/en/safety-and-securityabuse.

10 For example, Facebook increased the number of moderators who review content that potentially violates their community standards by 3,000 in 2017: S Gibbs, "Facebook live: Zuckerberg adds 3,000 moderators in the wake of murders" *The Guardian* (3 May 2017) available at: https://www.theguardian.com/technology/2017/may/03/facebook-live-zuckerberg-adds-3000-moderators-murders.

11 For example, in March 2018, the European Commission issued a Recommendation for enhancing the responsibility of online platforms in removing illegal online content: European Commission, "Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online", Brussels 1177. See also L Scaife, "The interrelationship of platform providers and users in the regulation of Twitter and offensive speech – is there a right to be offensive and offended at content?" (2013) 18(4) *Communications Law* 128.

1.22 These are important issues, but not ones which the Law Commission has been tasked to consider in this review.

1.23 We discuss the role of internet platforms at various points in this Report – notably in Chapter 2, which sets out contextual considerations concerning the online environment. However, in order to maintain our core focus on the criminal liability of individual perpetrators of abuse, and consistent with our Terms of Reference, we make no comment or recommendation about how the law might be reformed in relation to the criminal or civil liability of internet platforms.

1.24 The subject matter of this review – individual criminal responsibility – is therefore merely one component of a wider Government approach to online safety, and our recommendations should be considered in this context.

THE STRUCTURE OF THIS SCOPING REPORT

1.25 In Chapter 2, we outline how online communication works and the difficulties that the online environment presents to the criminal justice system generally. Key prosecution challenges include jurisdictional and enforcement difficulties, technical challenges and the scale of offending.

1.26 In Chapter 3, we identify the impacts of abusive and offensive online behaviour, both on victims and on society more widely. We assess whether the nature of harm caused by online abuse is different to the harm caused by offline abuse, and identify some characteristics of abuse which may mean that a victim may be subject to more, and aggravated, forms of harm from online offending in some circumstances.

1.27 In Chapter 4, we discuss the specific communications offences contained in the MCA 1988 and CA 2003, and analyse the protection this legislation provides to the online user.

1.28 In Chapters 5 to 12, we set out various criminal forms of abusive and offensive behaviour by broad categories of conduct, for example harassment and stalking, the making of threats, and abuses of personal privacy. We analyse the criminal law which applies to each set of behaviours and then suggest some of the challenges posed in applying the existing criminal law to online communications.

1.29 The behaviours and offences we examine in Chapters 5 to 12 are:

- Gross offensiveness;
- Obscenity and indecency;
- Threatening communication;
- Harassment and stalking;
- Hate crime;
- Privacy offending and disclosure without consent;

- False communications; and

- Inchoate offences (such as encouraging and assisting crime, and conspiracy).

1.30 We have collated and published online a comparative analysis of the way that some different jurisdictions have structured their offences relating to abusive and offensive online communications. We asked an expert from each region to assess whether their respective jurisdiction has achieved parity of treatment between offences committed online and offline. The jurisdictions covered are Australia, Ireland, Germany, New Zealand and Canada. We chose these jurisdictions because of their comparability with the context of England and Wales, and their different approaches to law reform in this area.

1.31 We conclude this Scoping Report with a Chapter that sets out our suggestions for the structure of Phase 2 of this project. The key further areas of work we recommend are:

- reform and consolidation of the communications offences, so that they are clearer and more proportionate;

- consideration of how the criminal law may more effectively address the specific harm caused to an individual who is subjected to a campaign of online harassment; and

- a review of how effectively the criminal law protects personal privacy online.

1.32 These recommendations are not provisional proposals or reform recommendations in themselves. Rather, they indicate areas where future consultation and policy development should be considered.

THE TECHNOLOGICAL DEVELOPMENTS WHICH HAVE LED TO THIS REVIEW

1.33 Bullying and verbal abuse, causing offence and thereby inflicting pain and suffering are, unfortunately, common features of human social interaction. As new methods of communication have developed, new tools have often been used to perpetrate abusive and offensive behaviour.

1.34 Until recently, communication has been naturally limited by the speed at which any message could be physically conveyed. Before the 19th century, the time taken to deliver any communication was constrained by the maximum speed of whatever was physically transporting it; whether that was a messenger, horse, bird or ship. Consequently, single messages inevitably had limited immediate reach.

1.35 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.

1.36 The new technological developments presented enhanced opportunities to disseminate abuse. In England and Wales, the criminal law responded accordingly.[12] For example, in response to the opportunity presented by a nationalised postal service, the Post Office Protection Act 1884 criminalised the sending of grossly offensive material by post.[13] Subsequently, section 10(2)(a) of the Post Office (Amendment) Act 1935 introduced a prohibition on using telephones to communicate indecent, obscene or menacing messages.

1.37 New mediums, through which harms are perpetrated, continue to challenge the currency of the law relating to communications offences. For example, in 1985, we recommended that a specific criminal offence be created for "poison pen letters", which had not yet been captured by the law.[14] A specific criminal offence was only created by section 1 of the MCA 1988.

The internet age

1.38 This trend has continued. The development of the internet has caused a seismic shift in the way that we communicate as a society, and brought with it the potential for harm and offence on a huge scale. However, only recently have criminal offences relating to abusive and offensive communications begun to be drafted to cater for the internet era. Even amongst these, such as section 127 of the CA 2003, the constituent elements of this offence draw heavily on pre-internet offences, such as section 10(2)(a) of the Post Office (Amendment) Act 1935.

1.39 This Scoping Report analyses the types of abusive and offensive behaviour that can be perpetrated online and asks whether the current criminal law is sufficient to provide the same protection to online victims as offline victims. There are, however, further fundamental questions that would need to be considered in Phase 2 of this project. As Chapter 2 will outline, many people behave differently "online" from how they behave "offline". The criminal law's response may need to cater for such difference, identifying the fundamental values that need to be protected while ensuring that the criminal law is the most appropriate, proportionate and effective means of doing so.

Social media and technology

1.40 Over half the world's population now have access to the internet[15] and spend, on average, one third of the time they are awake using internet enabled devices and

---

12 For further reading, see EH Freeman, "The Telegraph and Personal Privacy: A Historical and Legal Perspective" (2012) 46(6) *The EDP Audit, Control, and Security Newsletter* 9.

13 Other early regulation of communication included section 45 of the Telegraph Act 1863, which made it an offence punishable by a fine for any telegraph company employee (later British Telecom) improperly to divulge any message; and section 20 of the Telegraph Act 1868, which made it an offence for anyone having official duties connected with a telegraph company to disclose any telegraphic message contrary to their duty, punishable by imprisonment; see: *Hansard* (HL), 12 May 1981, vol 420, col 485.

14 Criminal Law: Poison Pen Letters (1985) Law Com No 147.

15 In 2018, over four billion people globally use the internet; see https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018. In 2017, 90% of households in Great Britain had internet access. For more information see Office for National Statistics, *Internet access – households and individuals*, Great Britain: 2017 (3 August 2017), available at

services.[16] Every 60 seconds, globally there are 156 million emails sent, 3.8 million search requests made on Google and two million minutes of calls made via Skype.[17]

1.41 Social media channels are now used by 75% of global internet users. Social media providers offer unprecedented ways to communicate instantaneously around the globe with billions of other people. This Report focuses on England and Wales, where social media use is similarly prevalent. The Office for National Statistics recorded that in 2017, 66% of United Kingdom adults were using social media sites. In the 16 to 24 age group, that figure rose to 96%.[18]

1.42 The traditional model of a named and identifiable individual "sender" and individual "recipient" which applied to many types of offline communication is not always a good fit with communication online.[19] Online communications via social media are often distributed anonymously, intended for more than one individual and are easily forwarded on to other people. Even where communications are sent online between named individuals, these people may be using pseudo identities and the traditional model may not apply.

1.43 It is hard to quantify the speed and scale of communication on social media because of the variety of different sites and providers. Latest studies suggest that around 500 million instant messages are sent per day on Twitter.[20] 1.47 billion people are daily Facebook users,[21] including around 44% of the United Kingdom population.[22] More than 40 billion messages a day are sent on WhatsApp, a free user to user and group messaging service.[23] On YouTube, a video hosting site, over 400 hours of video footage is uploaded every minute.[24]

---

https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2017.

16 See We are Social, *Digital in 2018: World's Internet Users Pass the 4 Billion Mark* (2018), available at https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018.

17 R Smith, *A million WhatsApp messages were sent in the time it's taken you to read this headline* (19 March 2018), available at https://www.weforum.org/agenda/2018/03/internet-minute-whatsapp-facebook-emails/.

18 Office for National Statistics, *Social networking by age group, 2011 to 2017* (24 August 2017), available at https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/adhocs/007401socialnetworkingbyagegroup2011to2017.

19 Though the sending of anonymous letters was undoubtedly an issue that predated the internet. In Chapter 4, we note that the Malicious Communications Act 1988 evolved specifically out of a concern to address the harm caused by "poison pen letters", but now covers a much broader array of harmful communications.

20 Amnesty International, *Toxic Twitter – A Toxic Place for Women* (March 2018), available at https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.

21 This was the average for June 2018, see https://newsroom.fb.com/company-info/.

22 See Statistica, *Forecast of Facebook user numbers in the United Kingdom from 2015 to 2022*, available at https://www.statista.com/statistics/553538/predicted-number-of-facebook-users-in-the-united-kingdom-uk/.

23 See Statistica, *WhatsApp Usage Shows No Signs of Slowing Down* (7 May 2018), available at https://www.statista.com/chart/13762/whatsapp-messages-sent-per-day/.

24 See Statistica, *Hours of video uploaded to YouTube every minute as of July 2015*, available at https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/.

1.44 Another interesting quality of social media is that whilst the minimal cost and accessibility of online communication encourages its users to share and comment on transient moments and experiences, many of those messages then become permanent records online, and are often publicly accessible. There is not necessarily that same permanence with offline communication. Even if the offline communication is in a permanent form, for example a letter in paper form, it will often end up in the sole control of the recipient.

1.45 In her speech announcing this project, the Prime Minister described social media as "one of the defining technologies of our age".[25] In doing so, she recognised the many positive qualities of communicating online, from sharing ideas, enabling campaigning on important issues and, more generally, allowing people to express themselves.

1.46 The Prime Minister also focused on some of the challenges of online communication, describing social media as a place of potential intimidation and abuse.[26] This echoes the words used in the latest Crown Prosecution Service guidance on charging offences involving communications sent via social media, which notes that "online activity is used to humiliate, control and threaten victims, as well as to plan and orchestrate acts of violence".[27]

1.47 That abuse is reflected in recent statistics. For example, in a 2018 Ofcom survey, 44% of social media users reported being deterred from posting content because of the potential for abusive comments or responses.[28]

THE GENDERED NATURE OF ONLINE ABUSE

1.48 Before taking on this project, we conducted a public consultation to ask whether this was a suitable project for us to undertake, as an independent, apolitical body. Consultees were overwhelmingly in favour of us doing this work and many of them shared with us their concerns about the operation of the current law and its perceived deficiencies.[29]

1.49 One of the concerns repeatedly raised about the current law was that women are disproportionately likely to be affected by online abuse. These concerns were echoed by the news cycle which simultaneously developed around offensive online communications during the 2017 election.[30] Anecdotally, we heard that the failure of the

---

25 The Rt Hon Theresa May MP, *Standards in Public Life* (6 February 2018), available at https://www.gov.uk/government/speeches/pm-speech-on-standards-in-public-life-6-february-2018.

26 The Rt Hon Theresa May MP, *Standards in Public Life* (6 February 2018), available at https://www.gov.uk/government/speeches/pm-speech-on-standards-in-public-life-6-february-2018.

27 Crown Prosecution Service, *Social Media - Guidelines on prosecuting cases involving communications sent via social media* (21 August 2018) para 43, available at https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media.

28 Ofcom, *Adults' Media Use and Attitudes Report* (25 April 2018), available at https://www.ofcom.org.uk/__data/assets/pdf_file/0011/113222/Adults-Media-Use-and-Attitudes-Report-2018.pdf.

29 This was one of the most widely supported projects suggested in our 13th Programme of Law Reform and received over 200 recommendations from stakeholders.

30 For further reading, see P Strickland and J Dent, Online harassment and cyber bullying, Briefing Paper (13 September 2017) HC 07967.

law in this area damages equality in numerous ways. Fears shared with us include concerns that:

(1) failing to combat abusive online communications allows behaviours to escalate into even more serious offline offending, such as stalking and physical abuse;

(2) failures in legislation mean that the police response is often confused and minimal, making it more likely that women will not report offending;

(3) persistent abusive online communications against women, children and other minority groups "normalises" behaviour of this kind, creating a society in which abuse against women and other minority groups could also go unchallenged offline;

(4) failure to legislate effectively against abusive online communications has a disproportionate economic impact on women, who feel unsafe on the internet and may disengage with the many opportunities it offers; and

(5) large-scale online abuse suffered by high-profile women may further erode the willingness of women to stand for elected public office, or to take up senior positions, reducing diversity in the workforce and public life for the next generation.[31]

1.50 In 2017, the United Nations Special Rapporteurs on Violence against Women and Freedom of Expression made a joint statement to highlight the many forms of gender-based attacks online. They said these included blackmail, threats of sexual assault, sexist comment, intimidation, stalking, surveillance and dissemination of private content without consent. They expressed their concern at how violence and abuse against women online can "chill and disrupt the online participation of women journalists, activists, human rights defenders, artists and other public figures and private persons".[32]

1.51 When Amnesty International surveyed women who said they had experienced some form of online harassment or abuse in the past year, more than a quarter (26%) had received direct or indirect threats of physical and sexual violence, and almost half (46%) had experienced abuse or harassment that was sexist or misogynistic in nature.[33] In that poll, 67% of women who had experienced abuse or harassment online in the United Kingdom said they had a feeling of apprehension when thinking about using the internet or social media. Our remit in this Scoping Report is limited to the law of England and

---

31 See, eg Inter-Parliamentary Union, *Sexism, Harassment and violence against women parliamentarians* (October 2016), available at https://www.ipu.org/resources/publications/reports/2016-10/sexism-harassment-and-violence-against-women-parliamentarians.

32 United Nations Human Rights: Office of the High Commissioner, *UN experts urge States and companies to address online gender-based abuse but warn against censorship* (8 March 2017), available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21317&LangID=E.

33 A Dhrodia, *Unsocial Media: The Real Toll of Online Abuse against Women* (November 2017), available at https://medium.com/amnesty-insights/unsocial-media-the-real-toll-of-online-abuse-against-women-37134ddab3f4.

Wales, but every indication is that these nationwide results are largely applicable and relevant in this jurisdiction.

1.52 The gender implications of abusive and offensive online communications were also highlighted in a report by the All Party Parliamentary Group ("APPG") on Domestic Violence, which recommended that we undertake this project. The APPG were concerned that the prevalence and impact of online abuse "risks undermining the significant progress made to tackle domestic abuse, and other forms of violence against women and girls, in recent years".[34]

1.53 In their report, the APPG observed the overlap between offline and online offending behaviour, stating that:

> Online abuse does not exist in the "virtual world" alone. Women experiencing domestic abuse are not only abused offline, but frequently harassed, abused and stalked online by their partners or ex-partners. This online abuse and harassment usually forms part of a pattern of coercive and controlling behaviour – which can encompass physical abuse, emotional and psychological abuse, financial abuse and sexual abuse. A Women's Aid survey of survivors of domestic abuse in 2013 found that 45% had experienced abuse online during their relationship. For 85% of survivors surveyed in 2015, this abuse was not only virtual – but perpetrated by a partner, or ex-partner, as part of a pattern also experienced offline.[35]

1.54 We have reflected these concerns by extending the range of offences we have analysed in this Report to include related offences, such as coercive control and stalking, which can be committed partly or wholly online.

STAKEHOLDER ENGAGEMENT IN PHASE 1

1.55 As this Scoping Report makes no substantive recommendations for reform, we did not hold a formal public consultation as we would do if we were suggesting any change to the law. However, in making an assessment of how the law works in practice, it was important that we understood the perspectives of those affected by it.

1.56 Stakeholders generously gave up their time and shared their experiences with us. They included victims and the charities which support them, Members of Parliament affected by this issue, representatives from the technology companies, the Crown Prosecution Service, lawyers, civil liberties groups and many others. We also liaised with government departments including the Department for Digital, Culture, Media and Sport, and the Government Equalities Office, as well as the London Mayor's Office for Policing and Crime. In total, we estimate we have asked more than 400 stakeholders

---

34 APPG on Domestic Violence, *Tackling domestic abuse in a digital age* (February 2017) p 24, available at https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/04/APPGReport2017-270217.pdf.

35 APPG on Domestic Violence, *Tackling domestic abuse in a digital age* (February 2017) p 6, available at https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/04/APPGReport2017-270217.pdf. See also Women's Aid, *Virtual World, Real Fear: Women's Aid report into online abuse, harassment and stalking* (February 2014) p 8, available at https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf.

for their views on this project or to share their experiences of the law in this area with us. We have held individual meetings or round table conversations with at least 150 people. We list some of these individuals in the Appendix to this report, and extend our thanks to them. Specific thanks must be extended to the Crown Prosecution Service, who contributed significantly to the workings of the Report by sharing their expertise and providing some of the prosecution data that we refer to.[36]

1.57 We extend our sincere thanks to Dr Micheál Ó Floinn, who has acted as an academic consultant on this project. Many other academics gave generously of their time and expertise either by reading drafts or chapters or attending meetings at the Law Commission. We thank them for their considerable assistance.

LOOKING AHEAD TO PHASE 2

1.58 Unsurprisingly, not everyone supports reform of the criminal law in this area. By way of illustration, even across Parliamentary Committees there is a divergence of opinion; for example:

(1) In 2014, the House of Lords Select Committee on Communications concluded that "the criminal law in this area, almost entirely enacted before the invention of social media, is generally appropriate for the prosecution of offences committed using social media".[37]

(2) In February 2017, the APPG on Domestic Violence identified "a compelling case for reviewing the legislative framework that deals with online forms of domestic abuse – to ensure it provides parity of protection between the online and offline worlds … The use of online technology to continue perpetrating abuse, coercion

---

[36] In relation to this data, the Crown Prosecution Service ("CPS") have asked us to make readers aware of the following:

The CPS collects data to assist in the effective management of its prosecution functions. The CPS does not collect data that constitutes official statistics as defined in the Statistics and Registration Service Act 2007. These data have been drawn from the CPS' administrative IT system, which (as with any large scale recording system) is subject to possible errors with data entry and processing. The figures are provisional and subject to change as more information is recorded by the CPS. Further caveats to consider in respect of these data are:

1. Offences recorded are those which reached a hearing. There is no indication of final outcome or if the charged offence was the substantive charge at finalisation.

2. Data relates to the number of offences recorded in magistrates' courts, in which a prosecution commenced, as recorded on the Case Management System.

3. Offences data are not held by defendant or outcome.

4. Offences recorded are those which were charged at any time and reached at least one hearing. This offence will remain recorded whether or not that offence was proceeded with and there is no indication of final outcome or if the offence charged was the substantive offence at finalisation.

[37] Social Media and Criminal Offences, Report of the House of Lords Select Committee on Communications (July 2014) HL 37.

and control must be barred through criminal and civil measures, in the same way as these behaviours are prohibited in the 'real world'".[38]

(3) In May 2017, a report by the Select Committee on Home Affairs, *Hate crime: abuse, hate and extremism online*, noted that "most legal provisions in this field predate the era of mass social media use and some predate the internet itself … The Government should review the entire legislative framework governing online hate speech, harassment and extremism and ensure that the law is up to date".[39]

(4) The Committee on Standards in Public Life published its review on *Intimidation in public life* in December 2017, and concluded the current criminal law dealing with online abuse on social media is sufficient and "should remain as it is".[40]

(5) In October 2018, immediately prior to the publication of this Scoping Report, the Women and Equalities Committee of the House of Commons published its report into *Sexual harassment of women and girls in public places*.[41] This report found that "online spaces are public places where sexual harassment of women and girls is rife" and looked forward to the Law Commission's analysis of the current criminal law in this regard.[42]

1.59 We understand from the stakeholder engagement we have carried out that this is a topic of interest to a large number of people with varying and strongly held opinions. We note, however, that we did not hear from any stakeholder who opposed us undertaking this initial phase of analysis, or who advanced the opinion that the criminal law ought not to apply to particular forms of abusive communication in the online space.

1.60 The Government has announced its intention to conduct Phase 2 of this project.[43] While we have identified a number of key issues that we consider should be addressed as part of this review, we recognise we will need to conduct thorough public consultation if any reform of the law is canvassed. We anticipate that the analysis of the current law in this Scoping Report will provide a foundation for any future consultation.

---

38 APPG on Domestic Violence, *Tackling domestic abuse in a digital age* (February 2017) p 4, available at https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/04/APPGReport2017-270217.pdf.

39 Hate crime: abuse, hate and extremism online, Report of the Select Committee on Home Affairs (May 2017) HC 609, p 19.

40 Intimidation in Public Life: A Review by the Committee on Standards in Public Life (December 2017) Cm 9543, p 60.

41 Sexual harassment of women and girls in public places, Report of the Women and Equalities Committee of the House of Commons (October 2018) HC 701.

42 Sexual harassment of women and girls in public places, Report of the Women and Equalities Committee of the House of Commons (October 2018) HC 701, p 35.

43 See HM Government, *Government response to the Internet Safety Strategy Green Paper* (May 2018) p 46, available at 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.

Chapter 2: The online environment

INTRODUCTION

2.1 As we explained in the introductory Chapter, one of the central aims of this Report is to assess whether abusive and offensive communications offences apply equally in the online environment as they do offline.

2.2 In order to make an effective assessment it is essential to have at least a basic understanding of the online environment. In this Chapter we provide that context.

2.3 First, we provide some basic technological background describing the development of the internet and the types of communications facilitated through it. This is intended to frame and inform the analysis in Chapters 4 to 12 of how criminal offences can be perpetrated in this environment.

2.4 Secondly, we will outline what and "where" this online environment is, and where abusive and offensive communications fit in taxonomies of "cybercrime".

2.5 Finally, we outline certain endemic challenges for domestic law enforcement in policing cybercrime. These challenges are broadly grouped into three areas: substantive criminal law challenges; investigative challenges; and social and regulatory challenges.

THE DEVELOPMENT OF THE INTERNET

Early origins

2.6 Given how transformative the internet has been for society, it is easy to forget how recent an innovation it actually is. In this section, we set out some of the key moments in its history and development.

2.7 As its name suggests, the internet is essentially an interconnected group of computer networks: the "network of networks".[1] While the historical evolution of the internet is complex, its origins are usually traced to the work in the 1960s of computer scientists studying "packet switched" networks.[2]

2.8 Simply put, "packet switching" is a way of breaking up the information in a communication into small units, transmitting them over networks of computers, and reassembling them at their destination(s).

---

1 Encyclopedia.com, *Network of Networks*, available at https://www.encyclopedia.com/computing/news-wires-white-papers-and-books/network-networks.

2 For detail see, eg JCR Licklider, *Memorandum for: Members and Affiliates of the Intergalactic Computer Network* (23 April 1963), available at http://worrydream.com/refs/Licklider-IntergalacticNetwork.pdf; JCR Licklider, "Man-computer symbiosis" (1960) HFE-1 *IRE Transactions on Human Factors in Electronics* 4; JCR Licklider and WE Clark, "On-line man-computer communication" (1962) *Proceedings of the Spring Joint Computer Conference* 113. See further B Leiner and others, "Brief History of the Internet" (1997), available at https://www.internetsociety.org/internet/history-internet/brief-history-internet/.

2.9 In the early 1970s, a number of different computer networks were developed enabling packet-switched networks, but they were often based on a diverse range of incompatible protocols and standards. The step that allowed these diverse networks to interconnect came in a paper published by Cerf and Kahn in 1974,[3] where they laid the foundations for the "Internet Protocol" ("IP") Suite or "TCP/IP". This suite basically comprised the conventions and standards used to define how each layer of the internet operated. It enabled internet communication by specifying how data should be split into packets, addressed, transmitted, routed and received.

2.10 Another technical innovation from this period, which is at the heart of all internet communications, is the Domain Name System ("DNS") which was created in the 1980s.[4] The DNS is a hierarchical decentralised naming system for computers connected to the internet, and is integral to everything from sending an email to accessing a website. One of its most important functions is to translate memorisable domain names (like google.com) into IP addresses, so as to facilitate interactions between devices. In this role, it basically operates like the internet's phone book, by providing a worldwide directory service for communications over the internet.

The internet and the "web"

2.11 The "World Wide Web" ("the web") and the "internet" are frequently confused and conflated in common parlance, but they are not the same thing.

2.12 As described at paragraph 2.7, the internet is basically the "network of networks" – a way of connecting computers together so they can exchange digital information.

2.13 The web, on the other hand, is an information space that is accessed through the internet. More technically, it has been defined as "an information space in which the items of interest, referred to as resources, are identified by global identifiers called Uniform Resource Identifiers ("URI")".[5]

2.14 For example, many of the people reading this Scoping Report will have accessed it through the web on our webpage. They will have connected to the internet through their Internet Access Provider, launched their browser, and typed "https://lawcom.gov.uk" (a URI). The browser will have displayed our webpage, and retrieved information from our home webpage. The reader will then click on a series of hypertext links to access this document.

2.15 The web is one way of being "online", a term which has come to be associated with any state of connectivity with the internet. However, it is only one of many ways of communicating with people and computers over this medium.

---

3 VG Cerf and RE Kahn, "A Protocol for Packet Network Intercommunication" (1974) 22(5) *IEEE Transactions on Communications* 637, available at https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf.

4 The DNS is largely credited to the work of Paul Mockapetris in 1983. For more information, see Internet Hall of Fame, "Paul Mockapetris", available at https://internethalloffame.org/inductees/paul-mockapetris.

5 W3C Technical Architecture Group, *Architecture of the World Wide Web, Volume One: W3C Recommendation* (15 December 2004), available at https://www.w3.org/TR/webarch/.

2.16 The internet and the web (in particular) are therefore relatively recent technological innovations. Concerns about abusive and offensive online communications are even more recent. As Ziewitz and Brown observe, for the early web pioneers "abuse and anti-social behaviour was not a concern, since all users at the time were part of a rather close-knit and trusted network of researchers and scientists from the same cultural background with a shared set of values and beliefs".[6]

Communicating over the internet

2.17 Below we briefly outline some of the more common ways of communicating with people and computers over the internet: website browsing, email, and social media.

2.18 This is a very simplified description of how these technologies operate, and will not need to be read by those that already have a basic understanding of such communications.

Website browsing

2.19 When a person accesses a webpage, two main types of computers interact: a client (the reader's internet-connected device such as a mobile phone or laptop) and a server (a computer that stores the information accessed via webpages).

2.20 Each of these computers will have what is called an "IP address" which is necessary for the computers to interact. For example, the Law Commission's IP address for the website is currently 52.56.64.229. If the reader had typed this into their browser, rather than the URI http://lawcom.gov.uk, they would also be able access the content of this webpage. However, readers are more likely to remember the latter, which is why the Domain Name System was developed in the first place.

2.21 Those operating a website will have arranged two key things: a domain name, and hosting facilities. For example, those who have a website ending in ".co.uk"[7] will have worked through a "registrar" to register a domain name with an organisation called Nominet.[8] They will also usually have used a web hosting service provider in order to "host" or "store" the content of the website on servers.[9]

2.22 A simplified version of what technically occurs in this example is as follows:

(1) The user connects to the internet using an Internet Access Provider such as BT or Virgin.

(2) They access a browser such as Google Chrome or Internet Explorer, which is a piece of software downloaded on their device in order to browse the web.

(3) They type "https://lawcom.gov.uk" into the browser.

---

6 M Ziewitz and I Brown, "A prehistory of internet governance", in I Brown (ed) *Research Handbook on Governance of the Internet* (2013) p 10.

7 ".uk" is referred to as a "country code top level domain", while ".co" is a second level domain. "Generic" top level domains, on the other hand, include ".com" and ".net."

8 For more information, see Nominet, *UK Domains*, available at https://www.nominet.uk/domains/our-domains/uk-domains/.

9 Unless the website owner is operating their own server.

(4) The browser sends a query out over the internet in response to the request to access the Law Commission's website, seeking to match the domain with its corresponding IP address.

(5) The first server that is contacted to resolve this query could be a DNS server operated by the Access Provider, which routes the request through other DNS servers and returns the relevant information.

(6) The browser sends a "Hypertext Transfer Protocol" ("HTTP") request to the web server over the user's internet connection using "Transmission Control Protocol/Internet Protocol" ("TCP/IP"), asking for the content of the webpage.

(7) The server then sends the relevant content from the website to the browser in small data packets, which are assembled by the browser and displayed to the user.

(8) The user's operating system on their device may "cache" the information about the web server in a temporary database, so that accessing the website will be faster next time.

2.23 The user in this example could also have accessed this information by first searching for a "hypertext" link to the Law Commission's website through a search engine such as Google. This linking of one web page to another is an important component of the web as an information space. Google alone currently processes 3.5 billion such requests every day.[10]

Email

2.24 The term "email" means "electronic mail".

2.25 Sending an email requires an email "client" that allows for the sending and receipt of emails. This could be in the form of a "webmail" service accessed through a user's browser, or a desktop or mobile phone application.

2.26 The essential features of an email client will:

(1) show "message headers" of all of the emails a user receives, displaying who sent the email, the subject etc;

(2) let the user read the body of the email message; and

(3) facilitate the creation of new messages and send them over the internet.

2.27 To send an email, the user needs to know the intended recipient's email address, which will consist of a user name, followed by the "@" symbol and then a domain name like gmail.com. Email clients use mail servers to send and receive emails, and these will again rely on the DNS and IP suite, using specific protocols such as the Simple Mail Transfer Protocol ("SMTP"), Post Office Protocol 3 ("POP3"), and Internet Message

[10] Internet Live Stats, *Google Search Statistics*, available at http://www.internetlivestats.com/google-search-statistics/.

Access Protocol ("IMAP"). These play different roles in the sending and receipt of email messages from remote mail servers.

2.28 It is estimated that in 2018, approximately 281 billion emails are sent per day,[11] though a large portion of this figure will comprise "spam" or "junk" emails which are unsolicited messages sent in bulk.

Web 2.0 and social networking

2.29 The web has developed rapidly since it was created in the 1990s, and some have tried to characterise the current state of development as "Web 2.0". The term Web 2.0 was coined by DiNucci in 1999,[12] and though contested,[13] 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.

2.30 Examples of Web 2.0 include social networking sites, online gaming, and news websites which allow users to comment on current affairs.

2.31 Social Networking Services ("SNSs") come in various forms, with a variety of features, but have been broadly described as "online communication platforms which enable individuals to join or create networks of [friends or] like-minded users".[14]

2.32 They share characteristics including users being invited to provide data to generate a "profile", and to share information such as status updates, videos, photographs, and music, so as to facilitate interaction with other users.[15] Essentially, SNSs "'bring together pre-existing interactive technologies on a single service', such as search, email, messaging, chat, blogs, gaming, discussion forums, VoIP [Voice over Internet Protocol], photos, music and videos".[16] Members' profiles are typically password protected, and users can normally configure privacy settings for their profile or parts thereof; material

---

11 H Tschabitscher, "The Number of Emails Sent Per Day in 2018 (and 20+ Other Email Facts)" (9 September 2018), available at https://www.lifewire.com/how-many-emails-are-sent-every-day-1171210.

12 D DiNucci, "Fragmented Future" (1999) 53(4) *Print* 32.

13 The term is contested by Sir Tim Berners-Lee, who has referred to it as a "piece of jargon", stating that "nobody even knows what it means". S Laningham, *developerWorks Interviews: Tim Berners-Lee* (22 August 2006), available at https://www.ibm.com/developerworks/podcast/dwi/cm-int082206txt.html.

14 EU Directive 95/46/EC, Article 29 Data Protection Working Party (DPWP), *Opinion 5/2009 on online social networking* (12 June 2009) p 4, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf. A judicial definition from the United States provides: "social networking websites allow visitors to create personal profiles containing text, graphics, and videos, as well as to view profiles of their friends and other users with similar interests": *LiveUniverse, Inc. v MySpace, Inc.* [2007] United States District Court, (CD Cal 4 June 2007), per Matz J. The European Commission has also defined social networking, and discussed some of the risks involved in using SNSs: European Commission, *Creating a Better Internet for Kids* (23 August 2018), available at https://ec.europa.eu/digital-single-market/en/content/creating-better-internet-kids-0.

15 EU Directive 95/46/EC, Article 29 Data Protection Working Party (DPWP), *Opinion 5/2009 on online social networking* (12 June 2009) p 5, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf.

16 G Warren, "Interactive online services, social networking sites and the protection of children" (2008) 19(7) *Entertainment Law Review* 165, p 165.

can be private, public or available only to "friends" or "followers". The extent and manner of protection depends on the SNS involved.

2.33 The number and variety of SNSs is enormous and growing rapidly. Some are used exclusively for particular interests or purposes. Flickr, for example, is a popular service for storing and sharing photos and videos, while "Youtube" is used exclusively for sharing the latter. Facebook is currently one of the most popular SNSs, with over two billion active users monthly worldwide.[17] Other popular SNSs include Twitter and Snapchat.

Twitter

2.34 Twitter was founded in 2006 and allows users that have registered a profile to send and receive messages, called "tweets", to a network of contacts; these messages can also be accessed by any web user if the profile is configured for broader public access, which is a default setting.

2.35 For over a decade, tweets were restricted to 140 characters, but this was doubled in 2017,[18] and users can now also share videos and pictures.[19]

2.36 Users will typically set up an account, and then follow other Twitter users, which basically subscribes them to receive updates of tweets by those users. Users can like, forward ("retweet") and reply to other people's tweets.

2.37 As each user could follow thousands of other people, they may only be updated by and read a small proportion of the tweets from their contacts. However, if you wish to draw someone's attention to a particular tweet, you can "mention" them, by including "@" and their username in the tweet; this ensures they get alerted to the tweet when they access Twitter. Private messaging to specific users is also possible on the platform.

2.38 Twitter can be accessed in numerous ways. Users can send a "tweet" from the twitter.com website, from a mobile phone application (a "messaging app"), or even through a standard SMS text message.[20] SNS users with smartphones frequently rely on messaging apps in order to communicate with friends, rather than SNS websites accessed via a browser, and some SNSs are only available as an app.[21]

2.39 A detailed explanation of how Twitter works was set out by Mr Justice Warby in an appendix to his judgment in *Monroe v Hopkins*,[22] a civil defamation claim that concerned

---

17 Statistica, *Number of monthly active Facebook users worldwide as of 2nd quarter 2018 (in millions)* (2018), available at https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

18 For all languages except Japanese, Korean and Chinese.

19 See Help Center, *How to share and watch videos on Twitter*, available at https://help.twitter.com/en/using-twitter/twitter-videos.

20 See Help Center, *How to Tweet via text message*, available at https://help.twitter.com/en/using-twitter/twitter-sms.

21 The term "app" is short for "application" and refers to software designed to run on specific mobile devices or tablets.

22 [2017] EWHC 433 (QB); [2017] 4 WLR 68.

untrue and defamatory statements made about the blogger Jack Monroe by journalist Katie Hopkins on Twitter.

Snapchat

2.40 One increasingly popular app is "Snapchat", which was created in 2011 and, as of February 2018, has 187 million daily active users.[23]

2.41 The main purpose of this particular SNS is the creation of multimedia messages called "snaps". Users can send contacts photos or videos, which can be edited to include comments, drawings, effects and filters, and new features are regularly added.[24]

2.42 One of the reasons why this messaging app became popular is that pictures and videos are only available for a short period of time, and essentially self-destruct once viewed by recipients.

2.43 Snapchat's current policy is that snaps are deleted from their servers once viewed by all recipients, and all unopened snaps are automatically deleted after 30 days. Snaps sent in a group chat are deleted within 24 hours if unopened.

2.44 However, there are methods through which users can save snaps, such as by taking a "screengrab" on their mobile device, which photographs the display and saves the image locally.

2.45 Where a user may have sent naked images of themselves (for example, sexualised "selfies"), thinking they will be deleted, these features have proved controversial and sometimes, devastating for the senders. Websites have sprouted where these covertly captured images are published. We discuss privacy offences and the non-consensual sharing of sexual images in Chapter 10.

2.46 Sometimes the capturing of a Snapchat image can help in the prosecution of a criminal offence. For example, in a recent case, the defendant had filmed and photographed her boyfriend after he had been stabbed. She shared a "snap" of the incident with her Snapchat contacts, with the caption "This is what happens when you fuck with me". One of her contacts captured the "snap" which was ultimately key evidence at her criminal trial where she was convicted of manslaughter.[25]

Instant messaging

2.47 Instant messaging ("IM") refers to a form of technology that allows users to communicate in near "real-time"; it is perceived as quasi synchronous like a telephone call or face to face conversation.

2.48 IM protocols vary, with some facilitating direct "peer-to-peer" communications, even allowing users to see one another's messages character by character as they are being

---

23 G O'Malley, "Snapchat App Users Grow to 187 Million", *Media Post* (6 February 2018) https://www.mediapost.com/publications/article/314149/snapchat-app-users-grow-to-187-million.html.

24 See, eg E Moreau, *Snapchat stories explained* (22 March 2018), available at https://www.lifewire.com/what-is-a-snapchat-story-3486000.

25 BBC, "'Snapchat queen' Fatima Khan jailed for killing boyfriend" (21 September 2018), available at https://www.bbc.co.uk/news/election-2016-london-45603199.

typed. Others operate on a client-server model where messages are first logged, and then retransmitted from the sender to the recipient. Many popular IM apps used today allow messages to be sent to users whether or not they are "online" at the time of sending; the messages will be delivered, and the recipient will be notified and can access them at any point thereafter.

2.49 SNSs like Twitter are sometimes viewed as a form of asynchronous communication and contrasted with IM apps, because the sender and receiver do not have to be "online" at the same time in order to interact. However, where both users are engaging on the platform more or less simultaneously, these distinctions become difficult to sustain.[26] Twitter now even facilitates "live" video streaming to followers,[27] while many other popular SNSs provide multiple forms of IM within their platform, including text, video and voice calls.

CYBERSPACE AND CYBERCRIME

2.50 In the last few pages we have attempted to capture and explain a small part of the online environment which is of relevance to this study. It is necessarily incomplete. The digitisation of society through the internet and computing is a hugely complicated transformation which cannot be captured in a few short pages.

2.51 The seemingly impenetrable complexity involved in understanding the online environment has encouraged the use of short and simple descriptors. A good example is "cyberspace". As with much of the popular language used around the internet, this descriptor is a deceptively simple label for a complicated and controversial technological concept.

2.52 This term was first coined in literature by William Gibson,[28] who described it as:

> a graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.[29]

2.53 Cyberspace quickly became a de facto synonym for the internet and the web, and suggested a digital dualism between this new virtual space and the "real world". Cyber-utopians and libertarians advocated it as a place where people could "go", "inhabit" and be set free from the rules of "real space" sovereigns. Barlow, for example, famously wrote a "Declaration of the Independence of Cyberspace" in 1996, warning governments to avoid this frontier:

> 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

---

26 M Nentwich and R König, *Cyberscience 2.0: Research in the Age of Digital Social Networks* (2012) p 52.

27 For more information, see Help Center, *How to create live videos on Twitter*, available at https://help.twitter.com/en/using-twitter/twitter-live.

28 The word first appeared in a short story: W Gibson, *Burning Chrome* (1982). It was later used in the novel: W Gibson, *Neuromancer* (1984).

29 W Gibson, *Neuromancer* (1984) p 128.

leave us alone. You are not welcome among us. You have no sovereignty where we gather.[30]

2.54 Early cyber-libertarians like Barlow, Johnson and Post[31] argued that States organised around traditional territorial structures could not, and should not, govern this new space; this would instead be done by the decentralised and self-regulatory efforts of "netizens". This argument was based on a number of assumptions, including that the networked environment destroyed the ability of States to control behaviour and generated legitimacy concerns, as some States would attempt to enforce laws to global phenomena.

2.55 These assumptions were quickly dismantled by other regulatory theorists, who identified numerous fallacies in this train of thought, most notably the assumption that cyberspace is a separate place.[32] While someone may think they are in a separate place when committing a criminal act, their corporeal self is still obviously in a physical "place" at the time of the act, and thus subject to criminal law enforcement. Equally, evidence in relation to this act might be thought to exist in a separate world or dimension, but it is of course bound up in our physical world, residing on the internet-connected devices and servers that were used. Indeed, this second-generation of internet thinkers pointed to the potential for governments to enforce laws through controlling the underlying "code".[33] Lessig has even argued that the online environment "has the potential to be the most fully, and extensively, regulated space that we have ever known — anywhere, at any time in our history".[34]

2.56 The debates between these theorists still endure to a certain extent. A police officer investigating a crime perpetrated over the internet would certainly be sympathetic to Post's arguments concerning the jurisdictional complexity which inheres in policing cyberspace. Post argued that "a world in which, on occasion, bullets are fired from one jurisdiction into another is not 'functionally identical' to a world in which all jurisdictions are constantly subjected to shrapnel from a thousand different jurisdictions".[35]

2.57 The concept of cyberspace, and its dualism between the "cyber" and the "physical", also endures, despite being a "myth" that fails to capture the blended reality of our digital world. [36]

---

30 JP Barlow, *A Declaration of the Independence of Cyberspace* (8 February 1996), available at https://www.eff.org/cyberspace-independence.

31 D Johnson and D Post, "Law and Borders – The Rise of Law in Cyberspace" (1996) 48 *Stanford Law Review* 1367.

32 See, eg, J Goldsmith, "The Internet and the Abiding Significant of Territorial Sovereignty" (1998) 5(2) *Indiana Journal of Global Legal Studies* 475.

33 JR Reidenberg, "Governing Networks and Rule-Making in Cyberspace" (1996) 45 *Emory Law Journal* 911; and, most notably, L Lessig, *Code and Other Laws of Cyberspace* (1999).

34 L Lessig, *The Laws Of Cyberspace: Draft 3* (3 April 1998) p 3, available at https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf.

35 DG Post, "Against 'Against Cyberanarchy'" (2002) 17(4) *Berkeley Technology Law Journal* 1365, p 1383.

36 PJ Rey, *The Myth of Cyberspace* (13 April 2012), available at https://thenewinquiry.com/the-myth-of-cyberspace/.

2.58 Nevertheless, for the purposes of this Scoping Report, the question of whether the cyber environment can be understood in spatial terms remains important. The elements of some criminal offences depend on physical concepts, like a "public place"[37] or physical "presence".[38] For our purposes, the question is therefore whether communications over the internet will always engage these criminal offences, and whether they are equivalent to acts and communications in other contexts from a substantive legal perspective.

Cybercrime

2.59 Related to the question of what is cyberspace, is the question of what is a "cybercrime". This is another commonly used term, but is again contested. Wall, for example, describes the term cybercrime as "meaningless", because of the tendency to use it without a scientific or legal signification.[39]

2.60 However, analysis of the concept of cybercrime is important for defining the parameters of this study and a number of basic distinctions can be made. First, we can distinguish between cybercrime and computer crime more generally. Walden, for example, argues that cybercrime is a subset of computer crime.[40] A computer or mobile phone need not be connected to the internet, but could be accessed without permission, with data copied or deleted. In this situation a criminal offence could have occurred (section 1 of the Computer Misuse Act 1990), but there would have been no "cyber" dimension to the offence.

2.61 A second basic distinction some make is between computer-focused or cyber-dependent crimes (offences only committed using computers and computer networks), such as unauthorised access to a computer system contrary to the Computer Misuse Act 1990, and computer-assisted or cyber-enabled crimes (conventional crimes that are facilitated and often rendered more effective with the advent of computing),[41] such as online fraud and online distribution of child sexual abuse images.

2.62 These basic distinctions do not, however, assist very much in terms of categorising the specific offences within the remit of the present review. Computer-assisted crime covers a huge swathe of the criminal law, and further delineation is required.

2.63 There are various other academic and legal taxonomies of cybercrime.[42] The classification scheme adopted for the present Report is driven by the categories of

---

37 Such as the common law offence of outraging public decency.

38 Such as some of the offences in the Public Order Act 1986.

39 D Wall, *Cybercrime: The Transformation of Crime in the Information Age* (2007) p 10.

40 I Walden, *Computer Crimes and Digital Investigations* (2016).

41 M McGuire and S Dowling, *Cyber crime: A review of the evidence – Research Report 75* (October 2013). The UK government has previously distinguished types of cybercrime in this way, See Serious and Organised Crime Strategy (2013) Cm 8715, para 2.54, available at https://www.gov.uk/government/publications/serious-organised-crime-strategy.

42 Gillespie for example categorises cybercrime into four categories: crimes against computers ("where the computer is the target of the crime"); crimes against property ("where the object of the cybercrime is to obtain property"); crimes involving illicit content ("where the crime related to the posting, hosting, or accessing of objectionable content"); and crimes against the person ("where technology is used as a 'weapon' against an individual, with the potential of causing harm to that person"). Using this taxonomy, the

"offline" offences that we have been asked to review: speech and communication offences which are abusive and/or offensive. The cybercrime offences analysed in this Scoping Report are thus a specific sub-set of content-related offence. This covers offences where individuals are targeted and harmed by abusive or offensive communications,[43] as well as speech and communications that have been criminalised for their inherent offensiveness, whether or not any individual has felt abused or insulted or has even received or read them.

ENDEMIC ENFORCEMENT CHALLENGES

2.64 The act of sending abusive and offensive communication is a not a new phenomenon. However, sending such communications over the internet can present unique challenges for law enforcement. Some enforcement challenges are offence specific while others apply more generally to all the offences we discuss in this Report. We set out some of these challenges here, and they will also be further illustrated in examples in subsequent Chapters.

2.65 General challenges in enforcing the current criminal law in relation to abusive and offensive online communications include:

(1) Balancing the application of the criminal law with the qualified right to freedom of expression.

(2) Working out where the offence is committed from a jurisdictional perspective.

(3) Dealing with the indeterminacy of the elements of offences as they apply to online communications.

(4) Dealing with investigative challenges presented by online communication.

(a) Getting access to evidence:

(i) when it is located outside England and Wales; and/or

(ii) when the offender is technologically capable.

(b) Technical capabilities and resources of the police.

(c) Role of the internet service providers (including social media).

(5) The scale of offending behaviour.

present review would cover some areas of the latter two categories. See A Gillespie *Cybercrime: Key Issues and Debates* (2016) pp 7 to 8. Another common categorisation is found in the Council of Europe's Convention on Cybercrime. The Convention divides cybercrime into four categories: computer-integrity crime, computer-related crime, content-related crime, and criminal copyright infringement. See Council of Europe, Convention on Cybercrime (2001) ETS No. 185.

[43] Walden suggests a further potential category of computer crime, which he calls "contact-related crime", "which focuses on the use of internet-related communication services, such as social media, as a means of contacting a person, whether directly [or] indirectly, in an abusive manner": see I Walden, *Computer Crimes and Digital Investigations* (2016) para 3.191.

(6) The characteristics of online communication which make abusive and offensive communication so prevalent.

Challenge 1: Deciding what to prosecute; balancing the application of the criminal law with the qualified right to freedom of expression

2.66 Article 10(1) of the European Convention on Human Rights ("ECHR") provides that:

> Everyone has the right to freedom of expression. This right shall include the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2.67 In *Handyside v UK*, the European Court of Human Rights ("ECtHR") stated that:

> Freedom of expression constitutes one of the essential foundations of [a democratic …] society, one of the basic conditions for its progress and for the development of every man. Subject to paragraph 2 of Article 10 … 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. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society".[44]

2.68 Article 10(2) describes the way in which the right to freedom of expression can be lawfully restricted. It denotes that the State can interfere with the right in Article 10 where it is for a legitimate aim, prescribed by law, and necessary and proportionate in a democratic society. A legitimate aim includes the prevention of disorder or crime, and the protection of the reputation or rights of others. Courts have interpreted this term "rights of others" to include a right not to be insulted by racist remarks.[45]

2.69 The existence, and protection, of Article 10 rights does not mean that all speech is protected. The ECtHR has drawn a line between protected and unprotected speech; the latter does not engage the right to freedom of expression in Article 10(1) in the first place.

2.70 In *Norwood v UK*, for example, an individual circulated a poster shortly after the 9/11 attacks which depicted the burning Twin Towers, with the text "Islam out of Britain – protect the British People". Norwood was charged with an aggravated offence under section 5(1)(b) of the Public Order Act 1986 (displaying, with hostility towards a racial or religious group, any writing, sign or other visible representation which is threatening, abusive or insulting, within the sight of a person likely to be caused harassment, alarm, or distress by it). He was convicted of the offence and applied to the ECtHR, claiming his Article 10 rights were infringed.

2.71 The case was found to be inadmissible, on the grounds of Article 17, which prohibits the abuse of rights in the ECHR. The ECtHR concluded that to entertain the case would amount to an abuse of the rights in the ECHR. It stated that "such a general, vehement

---

44 *Handyside v UK* (1976) 1 EHRR 737 at [49]. See also *Muller v Switzerland* (1988) 13 EHRR 212 at [33], reiterated in *Sunday Times v UK* (No 2) [1992] 14 EHRR 123.

45 *Jersild v Denmark* (1994) 19 EHRR 1.

attack against a religious group, linking the group as a whole with a grave act of terrorism, is incompatible with the values proclaimed and guaranteed by the Convention, notably tolerance, social peace and non-discrimination".[46]

2.72 The distinction drawn between protected and unprotected speech is controversial, as it is difficult to anticipate where the boundaries lie. Holocaust denial, for example, is an explicit offence in many countries, and the ECtHR has in some cases utilised Article 17 to dismiss freedom of expression arguments, with little examination of the claim and context.[47] This approach of the ECtHR has been criticised as it obviates the usual balancing which occurs when the Court assesses the right to freedom of expression, where Article 10(1) is engaged, and then the limitations that can be placed on speech in a particular situation, under Article 10(2).[48]

2.73 Recently, the Grand Chamber of the ECtHR has clarified – in the context of a holocaust denial case – that Article 17 will only apply "on an exceptional basis and in extreme cases [where] … it is immediately clear… that the impugned statements sought to deflect [Article 10] … from its real purpose".[49]

2.74 The Crown Prosecution Service ("CPS") Code for Crown Prosecutors in England and Wales instructs that prosecutors should only proceed with a prosecution for communications offences if interference with freedom of expression is "unquestionably prescribed by law, is necessary and is proportionate".[50]

2.75 In the context of some of the proscribed behaviours which we analyse in this Report, the line between the legal and the illegal, the protected and the unprotected, continues to be difficult to draw. As Scaife has observed, for example, if the right not to be grossly offended was enforced vigorously through the criminal law and applied to all social media posts, "it is likely that certain celebrity comedians would have their own personalised seat in their local magistrate's court for the contents of their Twitter pages".[51]

2.76 We discuss the difficulties the current criminal law on online abusive and offensive communications presents to prosecutors in subsequent Chapters of this Report.

---

46 *Norwood v UK* (2004) App No 23131/03.

47 For an analysis of the ECtHR's jurisprudence in this aspect, see P Lobba, "Holocaust Denial before the European Court of Human Rights: Evolution of an Exceptional Regime" (2015) 26(1) *European Journal of International Law* 237.

48 See, eg A Buyse "Dangerous Expressions: The ECHR, Violence and Free Speech" (2014) 63(2) *International and Comparative Law Quarterly* 491, p 496.

49 *Perinçek v Switzerland* App No 27519/08 (Grand Chamber decision, 15 October 2015) paras 114 to 115.

50 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (21 August 2018), para 27, available at https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media.

51 L Scaife, "The DPP and social media: a new approach coming out of the Woods?" (2013) 18(1) *Communications Law: Journal of Computer, Media and Telecommunications Law* 5, p 8.

Challenge 2: Working out where the offence is committed from a jurisdictional perspective

2.77 The sending and receipt of an abusive and offensive online communication will not necessarily happen within a single jurisdiction. Sometimes, for example, an offender will send a message from another country to a victim in this jurisdiction. Conversely, the illegal material may be published within this jurisdiction but only accessed abroad. Other messages may concern an individual in this jurisdiction, but may not have been sent through any computers here. They could, for example, be communicated in closed messaging groups between individuals based abroad, where none of the messages are stored or routed through servers in this country.

2.78 Crime perpetrated over the internet can therefore generate a number of difficult jurisdictional questions for substantive criminal law. In practice, however, domestic courts have developed broad legal approaches which facilitate the prosecution of offences where there are also foreign elements to the case.

How jurisdiction works for criminal offences – an introduction to the concepts involved

2.79 International law sets out the parameters for a State to regulate transnational criminal activity. It does so in three ways:

(1) prescriptive jurisdiction – this refers to a State's authority to establish the content and scope of criminal law in relation to particular situations;

(2) adjudicative jurisdiction – this refers to the authority of a State to apply law to persons or things, in particular through the processes of its courts;[52] and

(3) enforcement jurisdiction – this refers to the authority of a State to enforce its criminal laws and compel compliance.[53]

2.80 The multijurisdictional nature of many criminal offences perpetrated over the internet presents challenges for each of these jurisdictional concepts.

2.81 In this section, we outline the challenges which criminal offences committed online pose for the concepts of prescriptive and adjudicative jurisdiction, and begin by outlining international and domestic approaches to the concept of territoriality in the context of the criminal law.

---

52 See W Dodge, "Jurisdiction in the Fourth Restatement of Foreign Relations Law" (2017) 18 *Yearbook of Private International Law* 143, p 146.

53 See W Dodge, "Jurisdiction in the Fourth Restatement of Foreign Relations Law" (2017) 18 *Yearbook of Private International Law* 143, p 146; FA Mann, "The Doctrine of Jurisdiction in International Law" (1964) 111 *Recueil des Cours* 1; R O'Keefe, "Universal Jurisdiction: Clarifying the Basic Concept" (2004) 2(3) *Journal of International Criminal Justice* 735; and M Akehurst, "Jurisdiction in International law" (1973) 46 *British Yearbook of International Law* 145.

Territorial jurisdiction in international law

2.82 It has long been recognised that a State can exercise jurisdiction over conduct which constitutes domestic crimes and have been committed "in whole or in part"[54] within its territory.[55] In 1935, in an effort by the American Society of International Law ("ASIL") to codify international law, two separate territorial principles were identified within national legislation and jurisprudence. The first was the subjective principle, which provides jurisdiction when a crime was "commenced within the State but completed or consummated abroad".[56] The second was the objective principle, which provides a power to prosecute and punish when a crime was "commenced without the State but consummated within its territory".[57]

2.83 Although the issue of which of these States, if any, should enjoy priority was a topic debated in the literature at the turn of the last century,[58] by the time the ASIL drafted its Convention, it was realised that "the arguments were so evenly matched"[59] that neither, taken alone, could explain contemporary practice, and there was no reason for prioritising one over the other.[60] Thus, when any "essential constituent element"[61] was committed within a territory, that State could seize jurisdiction over the crime.

2.84 Today, international law continues to recognise both the subjective and objective principles of territoriality,[62] but they are not free from controversy, most notably because it is domestic law, rather than international law, that defines what the "constituent elements" of a crime are.

2.85 A variety of interpretations have emerged, particularly in relation to how the "effects" of criminal conduct are to be dealt with.[63] Often in the criminal context, the effects of a

---

54 "Draft Convention on Jurisdiction with Respect to Crime" (1935) 29(S1) *American Journal of International Law* 439, Draft Convention Article 3.

55 Concepts of extraterritorial jurisdiction are also recognised in international law, and envisage States prosecuting on the basis of factors such as the nationality of the offender. These concepts are not analysed further here, as statute has not provided for extraterritorial jurisdiction in relation to any of the offences under analysis.

56 "Draft Convention on Jurisdiction with Respect to Crime" (1935) 29(S1) *American Journal of International Law* 480, p 484.

57 "Draft Convention on Jurisdiction with Respect to Crime" (1935) 29(S1) *American Journal of International Law* 480, p 488.

58 M Akehurst, "Jurisdiction in International Law" (1972) 46 *British Yearbook of International Law* 145, p 152.

59 M Akehurst, "Jurisdiction in International Law" (1972) 46 *British Yearbook of International Law* 145.

60 "Draft Convention on Jurisdiction with Respect to Crime" (1935) 29(S1) *American Journal of International Law* 480, p 494.

61 "Draft Convention on Jurisdiction with Respect to Crime" (1935) 29(S1) *American Journal of International Law* 480, p 495.

62 C Ryngaert, "Territorial Jurisdiction Over Cross-Frontier Offences: Revisiting a Classic Problem of International Criminal Law" (2009) 9 *International Criminal Law Review* 187, p 189. See also C Ryngaert, *Jurisdiction in International Law* (2nd ed, 2015), Chapter 3.

63 In one United States case it was even said that "international law principles have expanded to permit jurisdiction upon a mere showing of intent to produce effects in this country…." *United States v Noriega*, 746 F Supp 1506 (SD Fla 1990), p 1513. For critique, see M Cherif Bassiouni, *International Extradition: United States Law and Practice* (6th ed, 2014) p 378.

crime will also form an element of the offence,[64] but some authors separate the effects and essential elements approaches.[65] According to Ryngaert, "international law seems to have satisfied itself with requiring that either the criminal act or its effects have taken place within a State's territory for the State to legitimately exercise territorial jurisdiction".[66]

Domestic territorial jurisdiction

2.86 The criminal law of England and Wales further complicates this picture, as it has developed a unique theory of jurisdiction which is distinct from the "constituent elements" approach common to many continental-European countries and the United States. The ambit of English criminal law has traditionally been strictly territorial. Unlike the legislative techniques of continental countries where criminal codes often contain the elements of the crime, and jurisdiction is dealt with elsewhere, the definition of a criminal offence in England and Wales normally includes its jurisdictional ambit. As Hirst notes, "misconduct committed outside the realm cannot ordinarily amount to the actus reus of an offence under English law".[67]

2.87 However, the English approach to cross-frontier offences does not fall straightforwardly within either the subjective or objective approaches to criminal jurisdiction. Even if some elements or effects of a crime are committed or felt within England and Wales, the offence may still not be regarded as having been "committed" within the territory.[68] The "terminatory" approach, as Glanville Williams labelled it, asks where the crime was completed, that is, where the last constitutive act takes place.[69]

2.88 The "constituent elements" approach, on the other hand, does generally accommodate the subjective and objective principles of territoriality. This is the dominant approach adopted by the States studied by Ryngaert,[70] and these States make full use of the flexibility afforded by international law in seizing criminal jurisdiction. This is done when either a constituent element of the offence, or its effects, occur within the jurisdiction,

---

64 In *S S Lotus (Fr v Turk)* PCIJ (ser A) No 10 (7 September 1927), and in an example provided by the ASIL, the consequences or "effect" of the criminal act were constituent elements (death being the consequence as well as an element of the criminal act of manslaughter and murder respectively). "Draft Convention on Jurisdiction with Respect to Crime" (1935) 29(S1) *American Journal of International Law* 480, p 502. See further U Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (2007) p 91.

65 See, eg M Akehurst, "Jurisdiction in International Law" (1972) 46 *British Yearbook of International Law* 145, pp 154 to 155.

66 C Ryngaert, "Territorial Jurisdiction Over Cross-Frontier Offences: Revisiting a Classic Problem of International Criminal Law" (2009) 9 *International Criminal Law Review* 187, p 188.

67 M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003) p 3. The "actus reus" is a Latin term which encompasses the act or omission that is the physical component of a crime (as opposed to the mental component).

68 M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003) p 113. See further C Ryngaert, "Territorial Jurisdiction Over Cross-Frontier Offences: Revisiting a Classic Problem of International Criminal Law" (2009) 9 *International Criminal Law Review* 187, p 193.

69 G Williams, "Venue and the Ambit of Criminal Law" (1965) 81 *Law Quarterly Review*, pp 276 to 288, 395 to 421, 518 to 538.

70 These include the US, France, Germany, the Netherlands and Belgium. See C Ryngaert, "Territorial Jurisdiction Over Cross-Frontier Offences: Revisiting a Classic Problem of International Criminal Law" (2009) 9 *International Criminal Law Review* 187.

and some States even assume jurisdiction on the basis of effects which do not form constituent elements of the crime.[71]

2.89 Both approaches present significant practical problems which have been exacerbated with the advent of cybercrime. The "terminatory" theory has the theoretical benefit of being a more conservative jurisdictional approach, thus limiting the potential for international conflict due to concurrent jurisdiction.

2.90 However, the restrictive nature of this approach has already come under pressure and has been abandoned domestically for offences such as trans-border fraud and dishonesty, in favour of a constituent elements approach. Moreover, the "terminatory" theory has been plagued by inconsistencies in application, with a variety of ways to manipulate its restrictive effect being found in the case law.[72]

2.91 The current approach of the courts of England and Wales has begun to move away from the "terminatory" theory, and the technical formulations which came within it when judges tried to identify where a crime was "completed" (although it is still a possible way of interpreting the ambit of an offence from a jurisdictional perspective).

2.92 The decision of Lord Woolf CJ in *R v Smith* remains the most authoritative statement of current practice, which envisages "jurisdiction if either the last act took place in England or a substantial part of the crime was committed here and there was no reason of comity why it should not be tried here".[73] This has been endorsed by the House of Lords,[74] and the "substantial" part/measure limb of this test applied in subsequent cases involving cybercrime, which will be discussed in subsequent Chapters.[75]

2.93 This additional limb adds substantially to the ambit of English criminal law, now reflecting quite an inclusionary approach to territorial jurisdiction. For example, the substantial measure test could allow for a prosecution in England and Wales where a victim in this jurisdiction is targeted from abroad, or where content is uploaded to the web from England and Wales.

2.94 However, the final example provided at paragraph 2.77 (sharing messages about a person in England or Wales, but with no domestic territorial nexus), illustrates the limits to even this broad approach. If the messages contained, for example, private sexual imagery, the sharing could be quite troubling for the victim, and an offence under section 33 of the Criminal Justice and Courts Act 2015 if "disclosed" in England and Wales.

---

71 M Akehurst, "Jurisdiction in International Law" (1972) 46 *British Yearbook of International Law* 145, 153. See further C Ryngaert, "Territorial Jurisdiction Over Cross-Frontier Offences: Revisiting a Classic Problem of International Criminal Law" (2009) 9 *International Criminal Law Review* 187, p 198.

72 See, eg discussion of *R v Keyn* [1876] LR 2 Ex Div 63 in C Ryngaert, "Territorial Jurisdiction Over Cross-Frontier Offences: Revisiting a Classic Problem of International Criminal Law" (2009) 9 *International Criminal Law Review* 187, pp 191 and 194 for United States examples. For further information see, M Goode, "The Tortured Tale of Criminal Jurisdiction" (1997) 21 *Melbourne University Law Review* 411, pp 427 to 429 and M Hirst, *Jurisdiction and the Ambit of the Criminal Law*, (2003) p 118 quoting *R v Ellis* [1899] 1 QB 230.

73 *Smith (Wallace Duncan) (No. 4)* [2004] QB 1418 at [57].

74 *Purdy v DPP* [2010] 1 AC 345 at 370.

75 See, eg *R v Sheppard and Whittle* [2010] EWCA Crim 65.

However, the sharing would be highly unlikely to constitute an offence here under either the "terminatory" or the "substantial" measure tests, without more.

The challenges in applying jurisdictional concepts to abusive and offensive communications offences committed online

2.95 As described in the previous paragraphs, the courts in England and Wales have recently tended to adopt broad approaches to territorial jurisdiction in the context of prosecutions of transnational criminal offences, but this does not mean that difficult questions around jurisdiction are avoided.

2.96 The ease with which activities in the networked environment can trigger the criminal laws of multiple countries simultaneously, would appear to make conflicts of jurisdiction an inevitability. Indeed, States can seek to prosecute offences on the basis of tenuous jurisdictional connections or in circumstances which other States would find disagreeable. This can cause inefficiencies, as multiple law enforcement agencies could, for example, invest resources in relation to the investigation of the same offence, and require further effort in the form of jurisdictional negotiations to determine where the offence should be prosecuted. It also carries considerable risk for the individual, who could face criminal prosecution in more than one country for the same act.[76]

2.97 Alternatively, the individual may face a "clash of laws", where countries both have a jurisdictional nexus, but differ on the legality of certain conduct or content. A person communicating "online" could be acting legally in one country, but illegally in another. If, for example, the enforcement of a criminal offence is based on factors such as the accessibility of website content in the latter country,[77] then that country's rules take priority, and the legality of the relevant internet communications become determined by the lowest common denominator. This also creates opportunities for individuals to operate or live in some countries, in order to frustrate laws in another.

2.98 The harmonisation of cybercrime laws in instruments like the Council of Europe's "Convention on Cybercrime" seeks to prevent such difficulties, by asking States to agree on areas of criminalisation and the basic elements of criminal offences. However, while many States have agreed to harmonisation in the context of certain cybercrimes, like those in relation to child sexual abuse imagery, it is more difficult to generate agreement in relation to the types of crimes under investigation in this study. States take very different positions on whether, for example, offensive communications should be a criminal offence, and even where there is general agreement, they may disagree on precisely how they should be defined. The United Kingdom, for example, has signed and ratified the Convention on Cybercrime, but has done neither of these in relation to the Additional Protocol to the Convention on the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[78]

---

76 For discussion of this issue within the context of the European Union, and the European Convention on Human Rights, see Micheál Ó Floinn, "The Concept of Idem in the European Courts: Extricating the Inextricable Link in European Double Jeopardy Law" (2017) 24(1) *Columbia Journal of European Law* 75.

77 See, eg *R v Perrin* [2002] EWCA Crim 747, as discussed in Chapter 6.

78 Although English law in this area, which we consider in Chapter 9, would already meet most of the criminalisation obligations in the Protocol. Moreover, other harmonisation initiatives are (currently) applicable

2.99 In subsequent Chapters, we illustrate how some of these jurisdictional challenges arise in the context of abusive and offensive online communication offences.

Challenge 3: Dealing with the indeterminacy of the elements of offences as they apply to online communications

2.100 Legal language can be indeterminate. It is sometimes ambiguous and vague.

2.101 Ambiguity arises in legal interpretation where "expressions have multiple meanings".[79] The word "person", for example, could refer to a human being as well a "legal person" (which can be, for example, a company).

2.102 Vagueness can also generate indeterminacy when, for example, it is unclear what types of properties something needs to possess in order to belong to a particular category. In this Scoping Report, we discuss concepts like "gross offensiveness", "obscenity", and "indecency" which are elements of offences that apply to abusive and offensive online communication. We note the lack of legal definition for these terms, and discuss the issues this may cause to victims and perpetrators alike, who may not know when a criminal offence has been committed. The vagueness of these concepts also causes interpretative challenges for police, prosecutors, judges and juries.

2.103 Vagueness can also be problematic for respect of rule of law values and principles such as predictability, consistency, equality, certainty, and non-retroactivity. If an offence contains vague language, then its practical application is often determined by prosecutorial discretion. If it is interpreted widely, as many of the vague concepts discussed in this Report are, then there is an increased likelihood that offences will overlap and their application will be confusing, difficult and uncertain.

2.104 All of this is not to say that vagueness in the law is always unhelpful. As the ECtHR has indicated, some vagueness is necessary in order to "avoid excessive rigidity and to keep pace with changing circumstances".[80] In this Report we highlight the vague terms that we think allow the law to respond effectively to new challenges, and those which lead to the problems of indeterminacy that we highlight in the paragraphs above.

Challenge 4: Dealing with the investigative issues presented by offensive and online abusive communications

Getting access to evidence located outside England and Wales

2.105 The phenomenon of "cloud" storage means that evidence of the commission of a criminal offence may be stored electronically and located overseas. This may be so even though the substantive crime took place in England and Wales. In such cases, there are concerns as to the adequacy of current investigatory powers for obtaining overseas evidence.

---

to the UK, notably, the EU's Combatting Racism and Xenophobia (Framework Decision 2008/913/JHA, 28 November 2008).

79 R Poscher, "Ambiguity and Vagueness in Legal Interpretation", in L Solan and P Teirsma (eds) *The Oxford Handbook of Language and Law* (2012).

80 *Kokkinakis v Greece* (1994) EHRR 397, para 40. Case law and judicial pronouncements assist to keep vagueness that is utilised in this way to acceptable limits for the purposes of the principle of legality.

2.106 The starting presumption is that, unless the contrary intention appears, statutes have territorial but not extraterritorial application.[81] The underlying principle, according with international comity, is that a State ought not to infringe the sovereign territory of another State.[82] That being said, the question of extraterritorially remains one of statutory construction, with any presumption being rebuttable. As a result, whether an investigatory power has extraterritorial effect depends on the wording of the provision in question, the statutory purpose and the relevant context.[83]

2.107 A key area in the investigation of offences relating to abusive and offensive communications relates to the powers of law enforcement to compel information from social media and other internet companies. While a country may place any number of onerous obligations on service providers based within its territory,[84] platforms that have no domestic presence have traditionally been thought not to be within the enforcement jurisdiction of the State. Some countries would even regard it as a criminal offence for law enforcement agencies from another country to compel information from service providers within their jurisdiction.[85]

2.108 There is evidence of direct international cooperation between United Kingdom law enforcement and service providers established abroad,[86] at least in relation to certain categories of data (like "communications data")[87] under the Regulation of Investigatory Powers Act 2000.[88]

2.109 However, these relationships are often insufficient for investigative purposes. Where other categories of data are involved (such as "content" data, for example, the content of a Facebook message) or where service providers otherwise refuse to cooperate, investigations can quickly come to a halt.[89]

2.110 In such situations, police need to resort to formal inter-State cooperation, such as through "Mutual Legal Assistance" Treaties ("MLATs"). This refers to the assistance that

---

81 *Masri v Consolidated Contractors International Co SAL* [2009] UKHL 43; [2010] 1 AC 90.

82 *Mackinnon v Donaldson, Lufkin and Jenrette* [1986] 1 Ch 482.

83 *R (KBR Inc) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin).

84 See, eg the Regulation of Investigatory Powers Act 2000.

85 Report of the Transborder Group, *Transborder access and jurisdiction: what are the options?* (Discussion Paper No T-CY 3, 2012) para 118.

86 See, eg Draft Communications Data Bill, Report of the Joint Committee on the Draft Communications Data Bill (2012-13) HL 79 and HC 479, paras 230 to 233, available at: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf.

87 See Regulation of Investigatory Powers Act 2000, s 21.

88 Cooperation was possible in relation to these categories of data due to the legislative framework in the United States which allows for the disclosure of customer records in certain situations. See 18 USC § 2702(c)(2).

89 On the difficulties of acquiring evidence from social media companies see, eg: Sky News, *Lucy McHugh murder: Facebook urged to give police access to suspect's account* (4 September 2018), available at https://news.sky.com/story/lucy-mchugh-murder-facebook-urged-to-give-police-access-to-suspects-account-11489888. Yvette Cooper MP, commenting on the case, noted "for there to be such long delays and cumbersome international processes for getting crucial information in such a serious case is deeply disturbing".

States provide one another in the investigation and prosecution of crime.[90] MLATs have long been viewed as an essential tool in the fight against transnational crime. However, they have several shortcomings; most notably, there may be a significant delay in a requested State dealing with a request for assistance.

2.111 Research suggests that responses to MLAT requests can take many months,[91] and there have been reports that police in the UK are sometimes waiting up to 18 months for evidence from social media companies.[92] The costs and effort required to gain access to evidence through this process will sometimes simply be prohibitive for law enforcement to pursue in the context of abusive and offensive communication offences.

2.112 More recently, States have legislated to address some of these jurisdictional issues. On 28 March 2018, the US Congress enacted the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), which permits, under certain conditions, non-United States law enforcement agencies to gain access to data held by United States operators. In the United Kingdom, the Crime (Overseas Production Order) Bill is currently making its way through Parliament. The Bill enables appropriate officers to apply for the production of existing stored electronic information located or controlled outside the United Kingdom.

2.113 If these new legal avenues become enforceable and are crafted and implemented in a way which is compatible with human rights and international law, this would allow for greater access to evidence from the major internet companies, who are often established in the United States. Many abusive and offensive communication offences which are of interest to domestic law enforcement will involve platforms such as Facebook, Twitter and Google.

2.114 These initiatives may therefore ameliorate some of the enforcement challenges faced by law enforcement, but they will not be a panacea. There will always be actors and service providers based abroad who refuse to cooperate, regardless of what the domestic powers purport to grant investigators.

Getting access to evidence when the offender is technologically capable

2.115 Evidence suggests that charge rates for offences (excluding fraud) are currently at 9% of recorded crimes in the year ending March 2018, despite the fact that the volume of crimes recorded is growing (now 4.9 million).[93]

---

90 C Nicholls and others, *The Law of Extradition and Mutual Assistance* (3rd ed, 2013) para 17.01.

91 K Westmoreland and G Kent, "International Law Enforcement Access to User Data: A Survival Guide and Call for Action" (2015) 13 *Canadian Journal of Law and Technology* 225.

92 F Hamilton, *Police wait 18 months for evidence from social media firms* (14 September 2018), available at https://www.thetimes.co.uk/article/police-wait-18-months-for-evidence-from-social-media-firms-6djhnwcj0.

93 Home Office, "Crime Outcomes in England and Wales: year ending March 2018" (Statistical Bulletin HOSB 10/18, July 2018) p 17, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729127/crime-outcomes-hosb1018.pdf.

2.116 In the area of malicious communications, which accounted for 11% of all recorded violence against the person offences in that year, the charge/summons rate was even lower than this, at 3%.[94]

2.117 Some of the reasons noted by the Home Office were that the perpetrator was not identifiable in 22% of cases, while the victim did not support police action in 46% of cases.[95] There are many barriers and difficulties in victims reporting these types of crime, and even when this is done, they may lose the courage and confidence to continue towards prosecution as the case develops.

2.118 It is interesting to note that in over one fifth of reported malicious communications offences, the perpetrator was not identifiable. Although we do not have a breakdown for how many of those offences were committed online, it is clear that the internet has provided numerous ways of effectively masking one's identity in the online environment.

2.119 First, individuals could rely on technologies to mask the identifying information that would typically be available when someone connects to the internet using their Internet Access Provider.

2.120 Connecting to the "Darkweb" through the "Onion Router" ("TOR") is one such way.[96] TOR was created by United States Naval Research Laboratory employees and other researchers with the purpose of protecting United States intelligence communications online. It basically conceals a user's location and internet usage from anyone conducting network surveillance, by directing internet traffic through a free, worldwide, volunteer overlay network consisting of thousands of relays. It is used by law enforcement, as well as individuals in repressed regimes,[97] and it is estimated that there are 62,165 TOR users based in the United Kingdom.[98]

2.121 However, like many internet technologies, it has "dual use", and it is also a haven for criminality. It is now commonly used for buying and selling illegal products (for example,

---

94 Home Office, "Crime Outcomes in England and Wales: year ending March 2018" (Statistical Bulletin HOSB 10/18, July 2018) p 15, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729127/crime-outcomes-hosb1018.pdf. It is not known how many of these offences applied to "online" malicious communications.

95 Home Office, "Crime Outcomes in England and Wales: year ending March 2018" (Statistical Bulletin HOSB 10/18, July 2018) p 15, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729127/crime-outcomes-hosb1018.pdf. It is not known how many of these offences applied to "online" malicious communications.

96 For a brief explanation of how onion routing works, see, eg Tor, *Tor: Overview*, available at https://www.torproject.org/about/overview.html.en.

97 Facebook has a "site" that is only accessible utilising TOR (facebookcorewwi.onion); this allows it to be accessed even in countries that try to block Facebook from local internet users.

98 See, eg Tor, *Users*, available at https://metrics.torproject.org/userstats-relay-table.html.

drugs and weapons) in criminal marketplaces and in the distribution of child sexual abuse imagery.[99]

2.122 Cases like that of Ross Ulbricht, who was convicted for operating a huge dark market place called the "Silk Road",[100] do suggest that users of TOR can be traced. However, these will likely only be the exceptional cases where considerable time and investigative resources have been expended – and where mistakes have been made by the perpetrators.

2.123 Technologies like Virtual Private Networks ("VPNs") can also serve to mask identifying information. VPNs have multiple important purposes in society. They are used, for example, by corporations and other organisations to ensure that employees or other trusted parties can gain access to internal computer resources over a safe and encrypted connection, even if the employees are accessing it through a less secure network (for example, the wifi in a café).

2.124 VPNs are now also readily available to members of the public; VPN software can be downloaded from a website, which will encrypt the data concerning users' browsing activity, even from the Internet Access Provider that is being utilised by the user. The VPN server basically acts as a third party, connecting to the web on behalf of the users. The websites that are accessed will see a connection (for example, an IP address) coming from the location of the VPN server, rather than the location of the user. This can frustrate any efforts by law enforcement to work with the owners of the website, where the VPN users may have committed offences. While the user in this scenario could be identified if the VPN service provider was subject to legal process, and responsive, some of these services are specifically created and orientated towards frustrating any such investigative efforts from law enforcement.[101]

2.125 Many websites and applications will also facilitate anonymous or pseudonymous communications. For example, Twitter allows people to use pseudonyms and does not have a "real name" policy like Facebook. In addition, many instant messaging applications now provide end-to-end encryption, meaning that even the app provider itself cannot "see" the communications. Some email providers are specifically advertised for sending "anonymous" emails,[102] and do not store IP address logs from its users or require any personal identifying information about them to set up an account.[103]

2.126 These sorts of protections are viewed by many as vital in order to prevent excessive and disproportionate surveillance by governments and other entities. However, cases like the Apple "San Bernardino" investigation illustrate the competing objectives and

---

99 See, eg HS Kassab and J Rosen, *Illicit Markets, Organized Crime and Global Security* (2018) pp 155 to 175. See also K Finklea, "Dark Web" (10 March 2017) Congressional Research Service Report 7-5700 p 9, available at https://fas.org/sgp/crs/misc/R44101.pdf.

100 N Bilton, *American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road* (2017).

101 They can do so by, for example, establishing servers in remote locations and in countries that do not have the necessary procedural powers to compel production of evidence from the VPN service provider.

102 See, eg http://www.sendanonymousemail.net/.

103 See, eg https://protonmail.com.

tensions that are at play.[104] The United Kingdom has recently intervened in this area in the form of section 253 of the Investigatory Powers Act 2016, which provides for the power to impose "technical capability orders" which can include "obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications data".[105] Whether such a power could be used to prevent an operator from providing end-to-end encryption services to its customers/users, was heavily debated during the passing of the Investigatory Powers Act 2016, but was not very clearly resolved.[106]

2.127 What this all suggests is that there is a constant "arms race" between criminals and law enforcement. Those that are committed to engaging in criminal activity over the internet will find ways of utilising technology to render their communications untraceable, or at least very difficult to trace. However, this issue is also likely to be more problematic in the context of some of the offences considered in this Report, rather than others. For example, those that are engaged in targeted campaigns of harassment against a particular victim may be more likely to invest time in learning about, and in utilising, the above technologies. In other areas, such as sending grossly offensive messages over the internet, individuals may put less thought into their communications, and engage in less planning; as a result, many of these communications will be more readily traceable to the sender.

Technical capabilities and resources and the response of the police.

2.128 The 2015 study of Digital Crime and Policing, by Her Majesty's Inspectorate of Constabulary ("HMIC"), suggested that police forces are facing numerous difficulties in investigating online crimes. Issues included the analysis of devices,[107] the numbers of trained digital media investigators,[108] knowledge in relation to the process for requesting

---

104 For discussion, see Electronic Privacy Information Centre, *Apple v. FBI*, available at https://www.epic.org/amicus/crypto/apple/.

105 Investigatory Powers Act 2016, s 253(5)(c). See also Investigatory Powers (Technical Capability) Regulations 2018/353.

106 G Smith, *Illuminating the Investigatory Powers Act* (22 February 2018), available at https://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html.

107 The delays and backlog in the analysis of devices cause many police forces to rely on private companies to analyse devices, sometime at huge cost to the force. As one senior officer stated: "we cannot afford backlogs and we cannot afford to outsource." See HMIC, *Real Lives, Real Crimes: A Study of Digital Crime and Policing* (December 2015) para 7.7, available at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf.

108 HMIC, *Real Lives, Real Crimes: A Study of Digital Crime and Policing* (December 2015) para 7.22, available at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf.

information from social media companies,[109] and generally, insufficient training and confidence in digital investigations.[110]

2.129 The study was also critical of inconsistency and deficiencies in some police responses to online offending. It compared the police's treatment of a typical offline crime with its response to the victim of a digital crime, saying the "contrast between their experiences could not be more stark … it is clear that there is some way to go before the victims of digital crime can be assured that they will receive the same response from the police as victims of more familiar crimes".[111]

2.130 This corresponds to what we have heard anecdotally. Some victims have suggested that the response from the police is not coordinated across the country and that the seriousness with which a complaint is handled may vary, depending on the technological capability of the force concerned and the type of offences committed. After experiencing trolling behaviour online, Stella Creasey MP said to the Guardian, "the police don't get it … unless they've said they want to rape or murder you".[112]

2.131 Chief Constable Stephen Kavanagh accepted the shortcomings in the police response to abusive and offensive online communications in his role as national police chiefs' lead on digital crime. He told the Today Programme in April 2016 that he did not think there was a single force across the UK "who think we have got this right at the moment". Chief Constable Kavanagh added in an interview with The Guardian that the police "need to step up and understand the quality of service to victims of these types of digital crimes is not good enough".[113]

2.132 His concerns included:

(1) The inability of the police to deal with the "sheer" volume of the offending behaviour – saying "the levels of abuse that now take place on the internet are on a level we never really expected. If we did try to deal with it all we would clearly be swamped".

(2) The lack of consistency across the forces when dealing with offences.

---

109 HMIC, *Real Lives, Real Crimes: A Study of Digital Crime and Policing* (December 2015) para 6.8, available at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf.

110 HMIC, *Real Lives, Real Crimes: A Study of Digital Crime and Policing* (December 2015) para 5.7, available at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf.

111 HMIC, *Real Lives, Real Crimes: A Study of Digital Crime and Policing* (December 2015) paras 3.50 and 3.55, available at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf.

112 R Mason, *Police and tech firms are failing to tackle trolling, says Stella Creasy* (15 April 2016), available at https://www.theguardian.com/technology/2016/apr/15/online-trolling-not-taken-seriously-enough-labour-stella-creasy.

113 S Laville, *Online abuse: "existing laws too fragmented and don't serve victims"* (4 March 2016), available at https://www.theguardian.com/uk-news/2016/mar/04/online-abuse-existing-laws-too-fragmented-and-dont-serve-victims-says-police-chief.

(3) The lack of knowledge across the forces – saying, "the challenge we have is to increase the level of knowledge and confidence around social hate crime in all officers, so they know how they can secure the evidence and what they need to do to investigate. They don't all know that at the moment".

2.133 Of course, the police are often the first to experience the limitations of the current communications legislation that we detail elsewhere in this Report. As Chief Constable Kavanagh said in a press interview in 2017:

> The trouble is that if you are a victim you need to understand how you articulate to the police what's concerning you. We have in the region of 30 pieces of legislation, some of them going back to the Offences Against the Person Act of 1861. The Computer Misuse Act is now 26 years old. That is not really helping investigators, the Crown Prosecution Service or victims to bring these people to justice.[114]

2.134 Chief Constable Kavanagh advocated reform of the legislation to rationalise the existing offences, saying:

> often victims don't know how to articulate what happened to them, they aren't clear what the offence is if there is one ... When they then get an ambiguous response from the police, it undermines their confidence about what has happened. It is not just about officers and staff being confident, it is about victims being confident that what has taken place is a crime. So the law needs to be pulled together and the powers consolidated into a single place.[115]

Role of internet service providers and online platforms

2.135 It is beyond the scope of this Report to consider the issue of online platform liability. Moreover, the regulation and governance of the internet more generally is a vast topic that we do not have scope to discuss in any detail here either. We will, however, highlight three important areas where service providers are frequently relied upon in the enforcement of abusive and offensive online communication offences, and some of the challenges that can arise in each area.

2.136 First, cooperation from service providers can be fundamental for investigations in terms of provision of data, for use as evidence in criminal trials. As noted, some inroads are being made here in the United Kingdom and the United States, but it will inevitably be an incomplete solution. Service providers based in other foreign jurisdictions, without any formal treaty arrangement with the United Kingdom, and who do not voluntarily respond to requests for data, could continue to frustrate certain criminal investigations.

2.137 A second way that service providers can be relied upon, particularly where the relevant website is abroad, and not responding to law enforcement requests, is to block access to infringing material through the internet access providers based in the United

---

114 M Weaver, *Police are inconsistent in tackling online abuse, admits chief constable* (14 April 2016), available at https://www.theguardian.com/uk-news/2016/apr/14/online-abuse-police-inconsistent-digital-crime-stephen-kavanagh.

115 S Laville, *Online abuse: "existing laws too fragmented and don't serve victims*" (4 March 2016), available at https://www.theguardian.com/uk-news/2016/mar/04/online-abuse-existing-laws-too-fragmented-and-dont-serve-victims-says-police-chief.

Kingdom. This type of filtering technology (for example, "Cleanfeed") was developed in order to prevent access to child sexual abuse imagery, through the work of the Internet Watch Foundation ("IWF"). However, it has since been expanded, through the courts, and is now also used to block websites involved in copyright and other IP law infringement.[116]

2.138 There are a number of ways of circumventing such blocks, including by utilising the VPN products described above. They would also be quite difficult to implement in relation to many of the types of criminal behaviour under analysis in the present Report. Websites that are blocked through the work of the IWF will often be clearly criminal, as they will involve child sexual abuse imagery relating to children. On the other hand, the legality of blocking access to a website for hosting "obscene" or "grossly offensive" content will be much more challenging, as the legality of the content itself may not be very clear. Clearly, if the remit of a body like the IWF were to expand to address broader categories of abusive and offensive communications, this would require a clear legislative mandate and legal framework for such blocking activities.

2.139 A third way that service providers can be relied upon is through the enforcement of their own rules and terms of service for their platforms. Many social media companies, in particular, have terms and/or community guidelines which will often (broadly speaking) cover most of the forms of abusive and offensive speech offences covered in this Report.[117] If the service providers are made aware of a breach of these terms, they can take certain actions, and these depend on the company's own policies and the type of breach involved. Common responses are for these platforms to remove the infringing content, or even suspend the infringer's account in more serious cases.

2.140 The platforms may take such action on the basis of user or law enforcement reports,[118] or often, on the basis of their own internal processes.[119] For some categories of unlawful material, machine learning and artificial intelligence ("AI") technologies can be quite effective at identifying and removing content (such as in the area of terrorist propaganda and hate speech), while technological processes like image hashing, can be effective at ensuring that child sexual abuse images or terrorist content are not circulated on platforms. These will be less effective at dealing with some of the other forms of abusive and offensive communication offences, given the often quite challenging qualitative process of interpretation that must be undertaken.

2.141 While the enforcement of terms and conditions in this way can obviously play a role in addressing abusive and offensive online communications, there are a number of

---

116 See, eg *Cartier International and Others v British Sky Broadcasting Ltd* [2016] EWCA Civ 658; [2017] 1 All ER 700. See also N Tusikov, *Chokepoints: Global Private Regulation on the Internet* (2017).

117 See, eg Facebook, *Facebook's Community Standards*, available at: https://en-gb.facebook.com/communitystandards/introduction.

118 Google, for example, has received 3675 requests for removal of content from United Kingdom law enforcement agencies since 2009, covering 115,547 items. 82% of these requests were complied with by Google. See Google Transparency Report, *Government requests to remove data*, available at https://transparencyreport.google.com/government-removals/overview?authority_search=country:GB&lu=authority_search.

119 See, eg Facebook, *Content Restrictions Based on Local Law*, available at https://transparency.facebook.com/content-restrictions.

limitations, concerns, and challenges, which include delays, hampering investigations, and a lack of transparency and impact on freedom of expression.

Delays

2.142 There are concerns with the timeliness of responses, and thus the effectiveness of responses. However, in our stakeholder meetings with social media companies, we heard evidence of some companies having relatively quick response times for content removal requests (for example, 24 hours) for most categories of abusive and offensive communications. This is particularly the case where they go through "trusted flagger" programmes with law enforcement agencies. Some of these companies have huge teams of reviewers employed for these purposes. Against that, however, we have heard of a number of reports from law enforcement and victims that there can be significant delays in responding to requests for removal. Smaller companies and platforms will obviously not have the same resources, and can sometimes take much longer to process such requests. In serious cases of victimisation in the context of abusive and offensive communications, delays like this can be devastating.

Hampering investigations

2.143 On the other hand, where these companies do act expeditiously in dealing with abusive and offensive communications on their platforms, there are possible risks and the danger of unintended consequences. Criminal investigations could be hampered if content is removed and deleted without the opportunity for law enforcement to first capture the relevant digital data for their investigative purposes.

Lack of transparency and impact on freedom of expression

2.144 Another concern relates to the interactions between law enforcement and service providers being too informal, insufficiently transparent, and with inadequate protections built into the process to ensure that, for example, the State agencies involved in requests for content removal/ "take down" are complying with their obligations to respect rights like the freedom of expression.[120]

Challenge 5: The scale of offending behaviour

2.145 Studies suggest that the penetration of social media use in the United Kingdom population is in the region of 66%, equating to some 44 million users.[121] Looking at the volume of online messages sent each day makes it immediately apparent that any sort of comprehensive law enforcement response will be hugely challenging.

2.146 Of course, much online communication is neither abusive nor offensive but bringing the criminal law to bear on the content which is, is made more difficult by the scale involved.

---

120 See, eg Article 19, *Self-regulation and 'hate speech' on social media platforms* (2018), available at: https://www.article19.org/wp-content/uploads/2018/03/Self-regulation-and-%E2%80%98hate-speech%E2%80%99-on-social-media-platforms_March2018.pdf.

121 Statistica, *Total number and the share of population of active social media and mobile social media users in the United Kingdom in January 2018* (2018), available at https://www.statista.com/statistics/507405/uk-active-social-media-and-mobile-social-media-users/.

Difficulties in making an accurate assessment of the scale of online abuse

2.147 Accurately quantifying the scale of abusive and offensive communication online is very difficult, let alone trying to draw a comparison with the scale of offline abuse. Conducting empirical research was outside the scope (and timeframe) of this Report and so, any numerical data in this Report comes from other studies and stakeholders.

2.148 It is hard to draw valid conclusions for the wider population from the data which exists. Data on the prevalence of online abuse is often commissioned in relation to specific subsets of the population, for example, children. Alternatively, many studies focus only on a specific type of online platform or a specific type of abuse, such as stalking or hate speech.

2.149 In some studies, including many on cyberbullying, it is unclear whether the offending behaviour being discussed would constitute a criminal offence under the criminal law, or whether the study is focused on generally unkind and unacceptable behaviour, which falls short of an offence but is capable nevertheless of causing harm. These concerns are perhaps reflective of the fact that there is no common language to describe internet behaviours – thus presenting another challenge in accurately categorising and measuring abusive and offensive communications.[122]

2.150 Drawing conclusions and trends from data is also complicated by the fact that the official recording of the behaviours that constitute crimes has not, historically, been particularly comprehensive. For example, the latest Office for National Statistics ("ONS") statistical bulletin for "Crime in England and Wales: year ending - March 2018" shows that the stalking and harassment sub-category rose by 30% compared with the previous year, accounting for almost one-third of the change in violence recorded by the police (30%; 68,307 offences).[123] ONS report that "it is likely that recording improvements are an important factor in this rise, particularly in relation to malicious communication offences due to improved compliance in recording of these new offences over time".[124]

2.151 Some of the major social media platforms publish regular "transparency reports". From the reports we have read, it is not possible to make an assessment, at a national level, of the extent of abusive and offensive communication originally made on any platform, or later removed from any platform. The reports are often compiled using global data and focus the analysis on specific categories. For example, a report might not give data

---

122 For a detailed discussion of some of these challenges see, eg S Livingstone and PK Smith, "Annual Research Review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age" (2014) 55(6) *Journal of Child Psychology and Psychiatry* 635.

123 Office for National Statistics, *Crime in England and Wales: year ending March 2018* (19 July 2018), available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018.

124 Office for National Statistics, *Crime in England and Wales: year ending March 2018* (19 July 2018), available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018.

on actual levels of abuse observed on the platform, but on the requests made through legal channels to delete prohibited content (a much lower figure).[125]

General conclusions on the scale of online abuse

2.152 Whilst acknowledging the challenges in quantifying precisely the levels of online abusive and offensive communication, the area has been the subject of a number of studies and more general conclusions can be drawn.

2.153 Some of the significant, and more recent, quantitative studies on this topic have included:

- Ofcom, *Adults' Media Use and Attitudes Report* (2018)[126] which found that close to half of internet users said they had encountered hateful content online in the past year.

- Demos*, The Scale of Online Misogyny* (2016),[127] looked at just under 1.5 million tweets globally over a period of 23 days in 2017 and (after discounting the 54% of tweets which were advertising pornography) identified 213,000 tweets containing aggressive uses of the word "slut" or "whore".

- Stonewall, *Hate Crime and Discrimination* (2017)[128] surveyed more than 5000 LGBT people across the United Kingdom and found 10% had experienced homophobic, biphobic and transphobic abuse or behaviour online in the last month. Over 26% of trans people had experienced transphobic abuse online.

- Ditch the Label, *In Game Abuse* (2017)[129] surveyed 2,515 young people aged 12 to 25 about their experiences of being subjected to, witnessing and perpetrating bullying in online gaming environments. They found that 57% had been bullied in an online game, 47% of young people said that they had received threats, and 40% had been subject to unwanted sexual contact.

- Amnesty International Global Insights, *Unsocial Media: The Real Toll of Online Abuse Against Women* (2017)[130] found that 46% of the women surveyed (all of whom had experienced some form of online harassment and abuse) had

---

125 We spoke with some of the major social media companies about the data they hold and whether it was possible to obtain more accurate figures to help quantify the levels of abusive and offensive communications on their platforms. We did not receive any additional data.

126 Ofcom, *Adults' Media Use and Attitudes Report* (25 April 2018), available at https://www.ofcom.org.uk/__data/assets/pdf_file/0011/113222/Adults-Media-Use-and-Attitudes-Report-2018.pdf.

127 Demos, *The Scale of Online Misogyny* (2016), available at https://www.demos.co.uk/blog/misogyny-online/.

128 Stonewall, *Hate Crime and Discrimination* (2017), available at https://www.stonewall.org.uk/sites/default/files/lgbt_in_britain_hate_crime.pdf.

129 Ditch the Label, *In Game Abuse* (2017), available at https://www.ditchthelabel.org/research-papers/ingame-abuse/.

130 A Dhrodia, *Unsocial Media: The Real Toll of Online Abuse against Women* (November 2017), available at https://medium.com/amnesty-insights/unsocial-media-the-real-toll-of-online-abuse-against-women-37134ddab3f4.

experienced sexist and misogynistic abuse. More than a quarter (26%) had received direct or indirect threats of physical and sexual violence.

- Safety Net*, Cyberbullying's impact on young people's mental health* (2018)[131] looked at the impact of cyberbullying on 11 to 25-year-olds. They found that 46% of young people surveyed had experienced threatening, intimidating or nasty messages via social media, email or text.

2.154 What is clear from the studies, and from the many qualitative reports we have received, is that online abuse is a widespread phenomenon in England and Wales. The internet facilitates the dissemination of abusive and offensive communications, and the targeting of victims, in many ways that would not be possible, or at least as easy, in relation to "offline" communications. This undoubtedly contributes to the scale of such communications, as found in the above studies.

Challenge 6: The characteristics of online communication which make abusive and offensive communication so prevalent

2.155 Studies, and the anecdotal examples that we have heard directly from victims and perpetrators of online abuse, suggest that a wide range of factors contribute to the prevalence of abusive and offensive communications online.

2.156 From a psychological viewpoint, the unique features of online communication make it more likely that people may send abusive and offensive messages:

(1) The offender may experience disinhibition in communicating with a victim who is often unseen and geographically remote. Citron has found that "people are quicker to resort to invective when there are no social cues, such as facial expressions, to remind them to keep their behaviour in check".[132]

(2) The offender may act in a way that he or she would not do offline, in the belief that he or she is anonymous online.

(3) The offender may also feel emboldened by acting alongside others who share a desire to communicate in an offensive or abusive way. Citron has noted that the internet has both "aggregative and disaggregate qualities":

> online, bigots can aggregate their efforts even when they have insufficient numbers in any one location to form a conventional hate group. They can disaggregate their offline identities from their online presence, escaping social opprobrium and legal liability for destructive acts.[133]

(4) The offender is more likely to be exposed to a range of abusive and offensive commentary which may have the effect of normalising that conduct for him or

---

131 A Chalk MP, The Children's Society and YoungMinds, *Safety Net: Cyberbullying's impact on young people's mental health, Inquiry report* (2018), available at https://www.childrenssociety.org.uk/sites/default/files/social-media-cyberbullying-inquiry-full-report_0.pdf.

132 DK Citron, *Hate Crimes in Cyberspace* (2014) p 59.

133 DK Citron, "Cyber Civil Rights" (2009) 89 *Boston University Law Review* 61, p 63.

her. The permanence of many forms of online communication means that any perpetrator who is looking for offensive content will find many examples of it.

The online disinhibition effect

2.157 There is an abundance of literature in psychology and related fields now attempting to understand how, and why, people act and speak differently when communicating "online" than they do "offline". In the 1990s, and early 2000s, it became so evident that this was a widespread phenomenon that it became an area of research in social psychology, and the term "the online disinhibition effect" was coined. The work of individuals like Suler has assisted to identify the different types of disinhibition, as well as the factors that contribute to it.

2.158 Suler distinguishes between two different types of disinhibition: benign and toxic disinhibition. The former might relate to situations where people share more information about themselves online than they normally would, or may even be more generous or caring when communicating over the internet, than they would "offline".

2.159 The second type of disinhibition is what Suler calls "toxic disinhibition". Here "we witness rude language, harsh criticisms, anger, hatred, even threats".[134]

2.160 Recent research also suggests that repetitive exposure to abusive and offensive communications can result in desensitisation to that form of speech offence.[135]

Ease of commission

2.161 From a practical standpoint too, it is also often easier for the offender to target people online than offline:

(1) The offender may be more likely to be able to identify a specific victim, or someone with the characteristics of the victim, because of the volume of personal information that is often available online.

(2) The offender is more likely to be able to target certain victims. In particular, high profile victims who would most likely be uncontactable offline, may have an active social media presence online which puts them within the offender's reach. Social media and email provide the victim with a ready mechanism for abusing a high profile victim, that would be harder to achieve through other means of communication.

(3) The offender can instantly communicate abusive and offensive communications from his or her own home, or any other location where he or she can access the internet. While it could be argued that the offender could similarly target victims via offline means at any time, for example by writing numerous poison pen letters or telephoning them from his or her own home, that argument does not adequately reflect the contribution that immediacy makes to the prevalence of online offending.

---

134 J Suler, "The Online Disinhibition Effect" (2004) 7(3) *Cyber Psychology and Behavior* 321.

135 W Soral and others, "Exposure to hate speech increases prejudice through desensitization" (2018) 44(2) *Aggressive Behavior* 136.

(a) Brown argues that the main distinguishing feature in the prevalence of online hate speech compared to offline, is the instantaneousness of the internet. He notes that the "the internet not merely facilitates, but also encourages, instant responses that are by their nature more spontaneous … [for example] … encouraging gut reactions, unconsidered judgments, off-the-cuff remarks, unfiltered commentary, and first thoughts, because they [in turn] encourage instant responses".[136]

(4) The offender knows that it requires comparatively minimal resources and effort to target multiple victims online versus offline. Yar has labelled information communication technology as a "force multiplier", recognising that it allows offenders quickly and easily to target victims across the globe, with a single offender able to reach thousands of targets.[137]

CONCLUSION

2.162 We have previously been reluctant to recommend criminal offences, "the commission of which could never be adequately policed".[138] This comment was made in the context of an analysis of whether offences for indecent or grossly offensive communications should be extended to all spoken messages, rather than only over particular communication mediums.

2.163 Today, we have similar concerns about the challenges which abusive and offensive online communications create for law enforcement. But what is certain is that there is an important role for the criminal law in this area; our stakeholders unanimously agreed that this was the case.

2.164 The ultimate focus of this work will therefore be to ensure that the criminal law is crafted in a way that applies to the online environment, and is suitable for the types of harms arising over this medium. Currently, as the following Chapters illustrate, it is failing in some respects.

2.165 There are clearly much broader social, educational, technical, legal, and regulatory issues to address, as outlined above, but the criminal law will certainly be an important cog in this machinery for dealing with abusive and offensive online communications.

---

136 A Brown, "What is so special about online (as compared to offline) hate speech?" (2018) 18(3) *Ethnicities* 297, p 304.

137 M Yar, "The novelty of 'cybercrime': An assessment in light of routine activity" (2005) 2 *European Journal of Criminology* 407.

138 Poison Pen Letters (1985) Law Com No 147, para 3.6.

Chapter 3: Impact on victims

INTRODUCTION

3.1 In Chapter 2, we discussed some of the ways in which abusive and offensive online communication can present new challenges from a technological and enforcement perspective. We also reflected on the characteristics of online communication which make abusive and offensive communication so prevalent.

3.2 This Chapter focuses on the impact of online abusive and offensive communication, with the aim of:

- identifying the impacts of abusive and offensive online behaviour, both on victims and on society more widely;[1] and
- assessing whether the nature of harm caused by online abuse is different to the harm caused by offline abuse.

3.3 Understanding the nature and seriousness of the harm caused is necessary to assess the adequacy of the protection provided by the current criminal law as outlined in Chapters 4 to 12.

OUR APPROACH TO THIS RESEARCH

3.4 Conducting empirical research was outside the scope of this six-month project. Instead, we conducted a range of stakeholder events and meetings with victims of online abuse and organisations who work with them. We have held a series of meetings with individual victims to understand more fully the range of abusive behaviours exhibited online, and the impacts these behaviours can have.

3.5 We also organised a well-attended stakeholders' experiences event, to which we invited victims of abusive and offensive communication, and the charities who support them, to participate in focus groups. Much of what we heard helped provide context, and jurisdiction specific examples, to the wealth of literature and psychological studies which already cover this topic.

3.6 Our work with stakeholders has reinforced the importance of looking at the impact of abusive and offensive online communications not just in relation to individual victims, but also within a wider societal context. We have seen that this abusive behaviour online can have a "ripple effect", impacting on not only the victim themselves, but on other people online, who witness the offending behaviour.

---

[1] We use the word "victim" as a term to denote the recipient of the abuse and for consistency with the other criminal offences discussed in this Report. We recognise that many of the people who spoke about their experiences to us would not use that label.

Drawing a distinction between online abuse and offline abuse

3.7 In examining the impact of online abuse we consider whether the nature of harm caused is different to harm caused by offline abuse.

3.8 In asking that question, we are not trying to minimise the scale, severity and impact of abuse in the offline world, nor are we suggesting that being the victim of abuse and offence in the offline world is any less harmful overall.

3.9 We have focussed on online abuse in this Chapter because it is a newer, and growing, phenomenon[2] and we felt it merited separate consideration in this Scoping Report.

3.10 Most victims of online abuse who spoke to us endorsed this approach and felt that online abuse, and the harms it caused, had not been properly addressed or understood in the same way as offline abuse.

3.11 Many individuals told us their experiences had led them to feel that online abuse was viewed as inherently less harmful than the offline equivalent. That is recognised also in the academic literature, where for example, as early as 2002, Herring notes that "cyber violence … tends to be viewed as less serious, less 'real' than violence in the off-line world". Her paper suggested that this might be because "cyber violence does not conform to our familiar prototype of violence in a number of respects", which included the fact that it was virtual rather than physical in nature.[3] We discuss the challenges which arise when online abuse is dismissed as something inherently less harmful than offline abuse from paragraph 3.71.

Recognising a degree of overlap between offline and online abuse

3.12 In exploring the impact of online abuse we accept that there may not be a clear cut division between online and offline abuse in some cases.

3.13 Studies suggest that a discussion of the impact of online abuse may appear artificial to some victims who experience both.

3.14 First, we know that some victims will be the recipient of abusive and offensive communications in both the offline and online world from different perpetrators.

3.15 For example, Awan and Zempi analysed the nature and impact of online and offline anti-Muslim hate crime and concluded that "in reality, online/offline boundaries may be more blurred than the terms imply", noting that "for victims, it is often difficult to isolate the online threats from the intimidation, violence and abuse that they suffer offline".[4]

---

2 See, eg the observations on changing behaviour over time, in S Livingstone and others, *Net Children Go Mobile: The UK Report* (2014) p 5 explains that "in 2010, 16% of children reported being bullied face to face, 8% on the internet and 5% via mobile phone. By 2013, this ratio had reversed, making cyberbullying (12%) more common than face-to-face bullying (9%)".

3 S Herring, "Cyber Violence: Recognizing and Resisting Abuse in Online Environments" (2002) 14 *Asian Women* 187, p 187.

4 I Awan and I Zempi, "The affinity between online and offline anti-Muslim hate crime: Dynamics and impacts" (2016) 27 *Aggression and Violent Behaviour* 1, p 1.

3.16 The Galop LGBT+ and Hate Crime Survey 2016 noted a similar blurring between being the victim of online and offline offending; 96% of respondents who reported experiencing online hate crime had also experienced offline hate crime.[5]

3.17 Secondly, online abusers may also be, or become, offline abusers. In perpetrating both forms of abuse, they may target the same victim or victims.

3.18 Academic studies have noted a degree of overlap between online and offline offending by the same perpetrator. A 2016 US study found that among the respondents who had been harassed online, 12% reported that their abuser had subsequently attempted to harm them in person.[6] The study concluded young women were particularly at risk; twice as many women in the under-30 age group reported an attempt to harm them offline – after online harassment – as men of a similar age.[7]

3.19 In a 2017 study of UK pupils aged 11 to 16 years old, 29% of the 2745 participants reported being bullied.[8] Only 1% of the study's participants said that they had been victims purely of online bullying. Researchers concluded that cyberbullying creates few new victims, but is mainly a tool to harm victims already bullied by traditional means.

3.20 The overlap between online and offline abuse was a subject explored by Women's Aid in their 2015 study of domestic violence victims. They found that for 85% of the respondents the abuse they received online from a partner or ex-partner was part of a pattern of abuse they also experienced offline.[9]

3.21 We were advised in similar terms by a charity who spoke to us about the impact of online stalking on victims. They told us:

> in stalking cases, online abuse will almost always be accompanied by offline crime. There is a risk in separating the two off too much and hiving off the prosecution of online in one area and leaving the offline elements. They have to be taken together.

3.22 Again, for those victims, drawing any distinction between the place in which the abuse occurred – whether on or offline – may feel overly simplistic. We acknowledge that for

---

5 As highlighted in M Stray, *Online Hate Crime Report 2017: Challenging online homophobia, biphobia and transphobia*, p 10, available at http://www.galop.org.uk/wp-content/uploads/2017/08/Online-hate-report.pdf.

6 A Lenhart and others, *Online Harassment, Digital Abuse and Cyberstalking in America* (November 2016) p 22, available at https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf.

7 A Lenhart and others, *Online Harassment, Digital Abuse and Cyberstalking in America* (November 2016) p 37, available at https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf.

8 D Wolke and others, "Cyberbullying: a storm in a teacup?" (2017) 26 *European Child & Adolescent Psychiatry* p 899.

9 See All-Party Parliamentary Group on Domestic Violence and Women's Aid, *Tackling domestic abuse in a digital age* (February 2017) p 6, available at https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/04/APPGReport2017-270217.pdf.

many people the impact of online abuse that we discuss in this Scoping Report may be further exacerbated by additional offline abuse.[10]

Recognising a degree of overlap between perpetrators and victims of abusive and offensive communications in some instances

3.23 We draw a general division in this Scoping Report between perpetrator and victim. Studies suggest, however, that some people's online lives may not be so clearly demarcated. For example, one recent review of cyberbullying research in young people found that in some studies there is "a strong link between being a cyber-victim and being a perpetrator".[11]

3.24 Failing to appreciate that a young person might be both an online perpetrator and victim, could result in missing signs which point to an increased risk of harm. As the study notes "this duality can particularly put males at higher risk of depression and suicidal behaviours".[12] Young perpetrators, under the age of 25, were around 20 per cent more likely to have self-harmed or attempted suicide than non-bullies.[13]

3.25 There is evidence that in some instances the perpetrator and the victim may in fact be the same person, raising the possibility of other issues of harm. A US study by Patchin suggests that a small, but significant percentage of adolescents have anonymously directed online aggression towards themselves, creating the erroneous impression that they are the victims of online abuse. This form of online behaviour has been labelled "digital self-harm."[14] It has been the subject of media attention in the United Kingdom when cyberbullying has been assumed to be a contributory factor in a suicide and then later discounted on the basis that the relevant messages were most probably authored by the deceased. This Report covers not only offences where individuals are targeted and harmed by abusive or offensive communications. It also deals with offences where speech and communications have been criminalised for their inherent offensiveness, whether or not any individual has felt abused or insulted or has even received or read them. We discuss the basis on which the law criminalises this type of behaviour in Chapter 5[15] but recognise that the descriptor of "victim" and "perpetrator" is not strictly accurate for the commission of such offences.

---

10 See the exacerbated psychological impact of being the victim of both online and offline abuse discussed in D Wolke and others, "Cyberbullying: a storm in a teacup?" (2017) 26 *European Child & Adolescent Psychiatry* 899.

11 A John and others, "Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review" (2018) 20(4) *Journal of Medical Internet Research* 129, p 11.

12 A John and others, "Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review" (2018) 20(4) Journal of Medical Internet Research 129, p 11.

13 A John and others, "Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review" (2018) 20(4) *Journal of Medical Internet Research* 129, p 9.

14 JW Patchin and S Hinduja, "Digital Self-Harm among Adolescents" (December 2017) 61(6) *Journal of Adolescent Health* 761, p 762.

15 See paragraph 5.11 onwards.

3.26 We acknowledge therefore at the outset of this Chapter that there are complexities in analysing the online environment through the traditional criminal law paradigm of perpetrator and victim and that sometimes the reality is more nuanced.

HARM CAUSED BY ONLINE ABUSE

3.27 The harm caused by online abuse can take many forms, including psychological and economic detriment.[16] The impact on victims can be devastating, even life threatening. Charities who work in this field have provided examples of people who have committed suicide after becoming the target of abusive and offensive communications online.

3.28 At the outset, it is important to acknowledge that not all victims have the same response to online abuse and offence, victims will often experience different "shades of harm".[17] For example, not every victim will react in the same way to reading a threatening message on Twitter; some may find it highly threatening, others will dismiss it. The most common reactions to online harassment and abuse captured in one US study were "annoyance" and "anger".[18]

3.29 What we have learned is that certain features of online communication appear generally to aggravate the harms caused to victims.

3.30 We have seen that specific harms resulting from being the recipient of abusive and offensive communication online can include:

(1) psychological effects and emotional harms;

(2) physiological harms; including suicide and self-harm;

(3) exclusion from public online space and corresponding feelings of isolation;

(4) economic harms; and

(5) wider societal harms.

---

16 In this Chapter, when we talk about "harm" we are specifically referring to the detrimental consequences experienced by victims, as a result of abusive and offensive online communication. For further discussion of harms see, eg J Feinberg, *The Moral Limits of the Criminal Law – Volume 1: Harm to Others* (1987). This focus does not serve to discount the potential for condemnation of forms of abusive and offensive communication on the basis that it is offensive conduct, without any directly visible consequences or victim. See, eg AP Simester and A von Hirsch, "Rethinking the Offense Principle" (2002) 8 *Legal Theory* 269.

17 C Langos, "Cyberbullying: The Shades of Harm" (2015) 22(1) *Psychiatry, Psychology and Law* 106, p 110.

18 See A Lenhart and others, *Online Harassment, Digital Abuse and Cyberstalking in America* (November 2016) p 44, available at https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf. 83% of victims felt annoyed, 68% reported feeling angry. In contrast 38% were worried, and 22% scared.

Psychological effects and emotional harms

3.31 The Government's Green Paper on the Internet Safety Strategy set out a wide range of psychological harms caused by online bullying and abuse, including anxiety and self-harm.[19]

3.32 Many victims told us that they had suffered significant emotional harm from their experience. Folami Prehaye, activist and Founder of Victims Of Internet Crimes (VOIC), whose sexual images were posted online without her consent, and viewed over 48,000 times, said: "I felt ashamed, disgusted, I used the term 'online rape'. This was how I felt, my pictures got a hell of a lot of views. I suffered anxiety, self-blame and depression".

3.33 Those types of psychological impacts were also documented in the Galop Online Hate Crime Report 2017, where participants reported a range of emotional responses to online hate crime including "shock, fear and anger". Participants described experiencing a deterioration in both mental and physical well-being, including sleep disturbances, depression, anxiety and paranoia.[20] The report goes on to note that whilst "the immediate acute impact usually lasted a few days or few months … many were left with a long-lasting sense of wariness and a heightened sense of threat".[21]

3.34 The psychological effects of online abuse may be particularly pronounced in children and young people. For example, research suggests that:

> Children who are cyberbullied are also at risk for negative outcomes such as loneliness, distress, loss or lack of friendships, lack of acceptance by peers, anger, lack of safety at school, low self-esteem, physical injuries, drug and alcohol use, weapons possession, and eating disorders…[22]

3.35 Victims may express a range of emotions including "anger, sadness, frustration, embarrassment, stress, fright, loneliness and depression".[23] Mitchell suggested that adolescent victims of digital abuse are more likely to show signs of depression than those who have never been victims of online abuse.[24]

---

19 Department of Digital, Culture, Media and Sport, *Internet Safety Strategy – Green paper* (October 2017), p 8, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf.

20 M Stray, *Online Hate Crime Report 2017: Challenging online homophobia, biphobia and transphobia*, p 12, available at http://www.galop.org.uk/wp-content/uploads/2017/08/Online-hate-report.pdf.

21 M Stray, *Online Hate Crime Report 2017: Challenging online homophobia, biphobia and transphobia*, p 16, available at http://www.galop.org.uk/wp-content/uploads/2017/08/Online-hate-report.pdf.

22 T Beran and others, "Children's Experiences of Cyberbullying: A Canadian National Study" (2015) 37(4) *Children & Schools* 207, available at https://tspace.library.utoronto.ca/bitstream/1807/74648/1/childrens%20experiences%20of%20cyber%20bullying.pdf.

23 S Livingstone and PK Smith, "Annual Research Review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age" (2014) 55(6) *Journal of Child Psychology and Psychiatry* 635, p 642.

24 KJ Mitchell and others, "The Relative Importance of Online Victimization in Understanding Depression, Delinquency, and Substance Use" (2006) 12(4) *Child Maltreatment* 312, p 315.

3.36 Some academics consider that communication technology is enabling new forms of psychological abuse to emerge. For example, Stephenson et al suggest that cyber partner abuse (also referred to as digital dating abuse) is a distinct new form of abuse.[25] It involves the use of technology, including text messages and social media to perpetrate abuse against a romantic partner. Such abuse might include verbal abuse, limiting social media access or trying to sexually coerce the victim. The authors point out that without the presence of social media, some psychologically abusive behaviours, such as "catfishing" would not exist.[26] As Gillespie notes, similar crimes of "romance fraud" are not a new phenomenon, but communications technology provides powerful new avenues to pursue this kind of behaviour.[27]

Physiological impacts

3.37 Some research suggests that online abuse has not only psychological impacts, but also physiological impacts on the victims. One recent national study, looking at the 21% of teachers surveyed in the Czech Republic who had been the subject of cyber attacks and, to a lesser extent, cyberbullying either in the previous 12-month period or prior, confirmed some victims suffered a range of physical symptoms. These included "sleep disorders, headaches, stomach-ache, lack of concentration or reduced immunity". In more exceptional cases (4 out of 1118 reported victims), responses included self-harm and suicide.[28]

3.38 In April 2018, researchers from the Universities of Oxford, Birmingham and Swansea conducted a systematic literature review of the last 2 decades of research, from over 30 countries, examining the association between cyberbullying involvement as a victim or perpetrator and self-harm and suicidal behaviour in children and young people.[29] The authors concluded young people (persons under 25 years) who were victims of cyberbullying were more than twice as likely to exhibit suicidal behaviour than non-victims.[30]

3.39 As Henry and Powell have observed, the data shows that "harms in the so-called 'virtual' world can have real effects, both bodily and psychical, and are not tangential, but increasingly central, to how individuals experience and live their everyday lives". They added that "the harms experienced by women in the sociospatial world may have at

---

25 V Stephenson and others, "Psychological Abuse in the Context of Social Media" (2018) 5(3) *Violence and Gender* 129.

26 Catfishing refers to a person pretending online to be someone that they are not, often with the intention of enticing the victim into a financial or sexual relationship or simply to bully or gain attention.

27 See A Gillespie, "The (electronic) Spanish Prisoner: Romance Frauds on the Internet" (2017) 81 *Journal of Criminal Law* 217.

28 K Kopecky and R Szotkowski, "Cyberbullying, cyber aggression and their impact on the victim – The teacher" (2017) 34 *Telematics and Informatics* 506, p 515.

29 A John and others, "Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review" (2018) 20(4) *Journal of Medical Internet Research* 129, p 1.

30 S Knapton, *Cyberbullying makes young people twice as likely to self harm or attempt suicide* (22 April 2018), available at https://www.telegraph.co.uk/science/2018/04/22/cyberbullying-makes-young-people-twice-likely-self-harm-attempt.

least as much impact on a person as traditional harms occurring against the physical body".[31]

Exclusion from the online space

3.40 Many victims told us that the advice they were given, when faced with large scale abuse of this type, was to remove themselves from the online space. This was seen as an unhelpful and inappropriate response to the offending behaviour of others. As one stakeholder told us, "removing yourself from the online world is extremely isolating. Online is a public space and can often be an extension of who we are".

3.41 As one US study put it:

> online harassment and abuse can impact [on] the relationships that victims have with friends, family, and work. Digital disruptions and abuse can yield a sense of increased isolation or disconnection from their communities for victims, whether because of the strain the harassment has put on their close relationships, or because their harassment has made them feel more cut off from avenues for communication and information-seeking.[32]

3.42 Liz Saville Roberts MP was critical of suggestions to victims that they should refrain from being online. At our stakeholders' experiences event she told us:

> when women are being abused online, the advice of the police can sometimes be to "not go online". That's the equivalent of telling women not to go out. What is being said online is not being considered as a threat. But if someone said it on the street, the police would act.

3.43 Research conducted by Bratu suggests that the removal of the victim from the online space is precisely the desired outcome of the offending behaviour. She noted that:

> … the stratagems used by trolls are instances of "silencing strategies". The latter endeavour to eliminate the persons from involvement in online public space, or discourage them from getting involved with additional public discussion. The media depiction and conceiving of trolling strengthen such "silencing strategies". Trolling categorises injured parties in a vulnerable condition and restricts freedom of expression ...[33]

3.44 Feelings of isolation can be exacerbated by the feeling that the situation is hopeless and that any attempt to resolve the issue may lead to more abusive and offensive

---

31 N Henry and A Powell, "Embodied Harms: Gender, Shame and Technology-Facilitated Sexual Violence" (2015) 21(6) *Violence Against Women* 758, p 765, see also the discussion of Sheila Brown's work on the integration by way of the "criminology of hybrids" in G Barak, *Criminology: An integrated approach* (2009), pp 318 to 321.

32 A Lenhart and others, *Online Harassment, Digital Abuse and Cyberstalking in America* (November 2016) p 47, available at https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf.

33 S Bratu, "The inexorable shift towards an increasingly hostile cyberspace environment: The adverse social impact of online trolling behaviour" (2017) 9(2) *Contemporary Readings in Law and Social Justice* 88, p 89.

communications. For example, studies show that often it is women who speak out about online abuse that receive more abuse.[34]

Economic harm

3.45 Citron observed that whereas new technologies have reduced the cost of engaging in socially destructive behaviour, "cyber-attack groups" have significant financial repercussions for victims, who:

> go offline or assume pseudonyms to prevent future attacks, impoverishing online dialogue and depriving victims of the social and economic opportunities associated with a vibrant online presence.[35]

3.46 Marshak sought to quantify the economic harms to victims of online harassment and offensive communication, who feel that they are increasingly excluded from the public space of the internet. She noted that:

> the steps the victim takes to protect themself can cause a significant economic impact, re-victimizing that person. Some costs are easily quantified, such as "legal fees, online protection services, and missed wages,"[36] … Others are harder to measure, such as business opportunities lost when clients fear that they will be targeted if they hire a victim. And, though difficult to assess, there is an opportunity cost to the time required to build the necessary paper trail – to prove stalking and harassment, to get police to pay attention, or to identify the perpetrator after a successful attack…[37]

3.47 Marshak looked specifically at the harm caused to female journalists who were the target of abuse as "it is relatively easy to measure the economic impact of harassment on journalists in online media, and their stories provide a good introduction to the problem". She found that:

> the effect of such harassment goes far beyond the personal impact on the journalists, who are "concerned for their personal security and in some instances [become] depressed and experience psychological trauma."[38] Some women adopted pseudonyms, and some dropped stories out of fear for their own safety, while others stopped reporting from certain regions or moved away, and sometimes left journalism entirely… Not only are global perspectives muzzled as journalists respond to harassment by writing less, but the disproportionate impact of online harassment on

---

34 See, eg EA Jane, "'Back to the Kitchen, Cunt': Speaking the Unspeakable about Online Misogyny" (2014) 28(4) *Continuum* 558.

35 DK Citron, "Cyber Civil Rights" (2009) 89 *Boston University Law Review* 61, p 62.

36 A Hess, *Why Women Aren't Welcome on the Internet* (6 January 2014), available at https://psmag.com/social-justice/women-arent-welcome-internet-72170.

37 E Marshak, "Online Harassment: A Legislative Solution" (Summer 2017) 54(2) *Harvard Journal on Legislation* 503, p 509.

38 A Barton and H Storm, "Violence and Harassment Against Women in the News Media: A Global Picture" (2014) 7 *International News Safety Institute and Women's Media Foundation,* available at http://newssafety.org/uploads/IWMF.FINALA.pdf [https://perma.cc/K35UHHWL.

> women means that some stories, which can only be told by women, are never shared.[39]

3.48 Marshak noted that the abuse has a longer-term impact on the opportunities available to these women, saying:

> on the business development side, online harassment campaigns can cause a different kind of negative economic impact by excluding victims from fora where critical contacts are made … Significant business opportunities are also lost if women who have been harassed follow all-too-frequent suggestions to limit their public exposure online, by making their accounts private and otherwise refraining from engaging in the social life of the internet.[40]

Wider societal harms

Identifying groups at risk of harm online

3.49 In Chapter 2 we explained that accurately quantifying the scale of abusive and offensive communication online is very difficult and set out the reasons why. Nevertheless, in looking at the wider societal harms caused by online abuse we acknowledge in this Chapter that, in some studies, some groups in society have been found to be the target of disproportionate amounts of online abusive and offensive communications. Amongst others, these include:

(1) women;[41]

(2) young people;[42]

(3) ethnic minorities;[43] and

---

39 E Marshak, "Online Harassment: A Legislative Solution" (Summer 2017) 54(2) *Harvard Journal on Legislation* 503, pp 509 to 510.

40 E Marshak, "Online Harassment: A Legislative Solution" (Summer 2017) 54(2) *Harvard Journal on Legislation* 503, p 510.

41 A Dhrodia, *Unsocial Media: The Real Toll of Online Abuse Against Women* (20 November 2017), available at https://medium.com/amnesty-insights/unsocial-media-the-real-toll-of-online-abuse-against-women-37134ddab3f4.

42 A Lenhart and others, *Online Harassment, Digital Abuse and Cyberstalking in America* (November 2016) p 35, available at https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf. See also, M Shan-A-Khuda and ZC Schreuders, *Characteristics of Victims of Cybercrime* (2017), The Cybercrime and Security Innovation Centre, Leeds Beckett University (unpublished), available at http://eprints.leedsbeckett.ac.uk/5074/1/Characteristics%20of%20Victims%20of%20Cybercrime.pdf.

43 See, eg D Abbott, *I fought racism and misogyny to become an MP. The fight is getting harder* (14 February 2017) available at https://www.theguardian.com/commentisfree/2017/feb/14/racism-misogyny-politics-online-abuse-minorities, B Tynes, *Online racial discrimination: A growing problem for adolescents* (December 2015) available at https://www.apa.org/science/about/psa/2015/12/online-racial-discrimination.aspx. See also generally the discussion in Hate crime: abuse, hate and extremism online, Report of the Select Committee on Home Affairs (2016-17) HC 609, available at https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/60902.htm.

(4) LGBTQ individuals.[44]

3.50 The plethora of studies on online abuse, often conducted in different jurisdictions on different time frames and looking at different subsets of the population, can make it hard to draw precise quantitative conclusions about the scale of abuse suffered by any particular group of people in this jurisdiction.

3.51 One of the issues with trying to determine absolutely how much abuse has been suffered is that the data set used may not reflect the full extent of offending behaviour. For example, Herring sets out a number of reasons why cyber violence might be underreported by women:

(1) "Violence, especially when it has a sexual component, tends to be underreported due to feelings of guilt or embarrassment";

(2) "Females, in particular, are taught to believe that they are somehow to blame if they are sexually aggressed; this social conditioning makes them less likely to report acts of sexual aggression";

(3) "A deeper problem is that violence against females is so widespread, and manifested in such diverse forms, that it is considered 'normal' by many females and males. Thus most teenage girls, if asked if they have ever been sexually harassed, are likely to respond 'no', but when asked specific questions, are able to report numerous harassment incidents, which they take to be simply 'the ways things are'".[45]

3.52 Also, it can be hard to find studies which address the numerical incidence of abuse and enable comparisons to be made.

3.53 To take abuse directed at women as an example, many women have shared with us detailed and upsetting accounts of the scale of abuse they have faced online. Much of the abuse described is sexist or misogynistic in nature. As Liz Saville Roberts MP told us: "there is so much online abuse geared towards women. Often it's about devaluing women or degrading them sexually".

3.54 In Chapter 1 we set out many of the concerns that have been raised with us about the impact of women being disproportionately likely to be affected by online abuse and the studies and reports which support that conclusion.

3.55 But we accept that, in recognising the online abuse and harassment of women, it is hard to draw precise conclusions about the scale of abuse suffered by gender. Often the situation can be more nuanced than that. For example, a US survey of internet users in

---

44 See, eg A Lenhart and others, *Online Harassment, Digital Abuse and Cyberstalking in America* (November 2016) p 38, available at https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf, which found, amongst other differences, that "almost half (49%) of LGB internet users say someone has tried to embarrass them online, more than twice the rate of heterosexual internet users (22%). 18% of LGB individuals report that someone has encouraged others to harass them online, compared with just 4% of those who are not LGB".

45 S Herring, "Cyber Violence: Recognizing and Resisting Abuse in Online Environments" (2002) 14 *Asian Women* 187, p 187.

2016 suggested that women were disproportionately likely to be victims of some specific forms of abuse. For example, it found that men were equally likely to suffer harassment online as women, but that harassment was of a different type with men, for example more likely to be physically threatened or called offensive names. It found that women were twice as likely to be sexually harassed online or be stalked online, as well as significantly more likely to have sensitive personal information exposed, or have rumours spread about them.[46]

The proportions of abuse directed at particular groups of people

3.56 As we acknowledge in Chapter 2, it is difficult to make an accurate assessment of the scale of abuse online.

3.57 However, as we discuss in the preceding paragraphs, it is possible to identify groups of people who seem disproportionately likely to experience some forms of online abuse. Studies also suggest that where a victim belongs to more than of the one groups listed in paragraph 3.49 they may find themselves a particular target for abusive and offensive communication online. For example, Weiser and Miltner coined the term "networked misogyny" to describe "an era that is marked by alarming amounts of vitriol and violence directed toward women in online spaces".[47] They note that these forms of violence are not only about gender, but are also often racist, with women from ethnic minorities as particular targets.[48]

3.58 The data from the US suggest that gender, when combined with other factors, such as age, can put women at higher risk of certain types of abuse. So, for example 20% of women aged 18 – 29 had reported sexual harassment online, compared to 5% of men.[49]

3.59 We have observed similar impacts in this jurisdiction. Amnesty reviewed nearly one million tweets sent in the run up to the 2017 general election. They discovered that Diane Abbott, a black female MP, received almost half of the abusive tweets sent to all female MPs in the period, 10 times more abuse than any other female MP. Other black, and Asian, female MPs received one third more abusive tweets than white female MPs.[50]

---

46 See A Lenhart and others, *Online Harassment, Digital Abuse and Cyberstalking in America* (November 2016), available at https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf, p 34. A 2017 United States research study, in contrast, concluded that men and women "differ modestly in the type of harassment they encounter online" with men being slightly more likely to experience any form of online harassment, see Pew Research Center, *Online Harassment 2017* (July 2017), p 7, available at http://www.pewresearch.org/.

47 S Banet-Weiser and KM Miltner, "MasculinitySoFragile: culture, structure, and networked misogyny" (2016) 16(1) *Feminist Media Studies* 171, p 171.

48 S Banet-Weiser and KM Miltner, "MasculinitySoFragile: culture, structure, and networked misogyny" (2016) 16(1) *Feminist Media Studies* 171, p 171.

49 A Lenhart and others, *Online Harassment, Digital Abuse and Cyberstalking in America* (November 2016) p 36 available at https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf.

50 See report at Amnesty International UK, *Black and Asian women MPs abused more online* (2017), available at https://www.amnesty.org.uk/online-violence-women-mps. Note that the report has been footnoted with the following caveat: "to increase accuracy, Amnesty staff reviewed a sample of the tweets labelled as abusive

3.60 Diane Abbott MP subsequently described the abuse she received after speaking about the online abuse in a parliamentary debate:

> My office got flooded with communications, both by letter and by email. People sent us emails and letters full of swastikas, people sent us postcards and letters with pictures of monkeys and chimps. People sent us hundreds of emails using the word nigg*r—that's the sort of response we get. It's highly racialised and it's also gendered because people talk about rape and they talk about my physical appearance in a way they wouldn't talk about a man. I'm abused as a female politician and I'm abused as a black politician.[51]

3.61 Sometimes the quantitative impact of abusive and offensive online communications in society is most easily illustrated by reference to a specific subset of online comment. For example, in 2016 the Guardian commissioned research into the 70 million comments that had been left on news articles on its site in the previous decade. They produced quantitative evidence that:

> Articles written by women attract more abuse and dismissive trolling than those written by men, regardless of what the article is about. Although the majority of our regular opinion writers are white men, we found that those who experienced the highest levels of abuse and dismissive trolling were not. The 10 regular writers who got the most abuse were eight women (four white and four non-white) and two black men. Two of the women and one of the men were gay. And of the eight women in the "top 10", one was Muslim and one Jewish. And the 10 regular writers who got the least abuse? All men".[52]

Impact of abuse directed towards people with certain characteristics

3.62 If online abuse is disproportionately directed towards certain groups in society then those groups may be deterred from using one of, if not the most, defining mediums of our age. Arguably, society itself suffers harm if sectors of the population are under represented online, or left unable to achieve their full economic and social potential.

3.63 There is also a risk that the scale of online offending risks normalising abuse and perpetuating further harm against minority groups.

3.64 Certainly, one of the attributes of online abuse is that it is often observed by others, which can be particularly concerning to onlookers who share the same characteristics as the victim. As another stakeholder told us:

> the snowballing of abuse online by multiple people on one victim is damaging to the victim but can also have adverse effects on unintended victims who fall within the same group as the victim if they witness this kind of abuse online, for example,

---

to better train the tool to learn and recognise what abusive tweets look like. We estimate our results are about 64% accurate".

51 Quoted in A Dhrodia, *We tracked 25,688 abusive tweets sent to women MPs – half were directed at Diane Abbott* (5 September 2017), available at https://www.newstatesman.com/2017/09/we-tracked-25688-abusive-tweets-sent-women-mps-half-were-directed-diane-abbott.

52 B Gardiner and others, *The dark side of Guardian Comments* (12 April 2016), available at https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments.

religion, race. Online abuse has a real impact on how these victims exist in the offline world. If you are targeted by a large group of anonymous abusers it can feel like it could be anyone on the street. If it is about religion, you cannot hide your hijab, so you change your offline behaviour, you stay in.

3.65 Internet users who have witnessed or experienced online harassment or abuse are significantly more likely to self-censor than those who have not.[53] Amnesty International found, for example, that around a third of women polled in a 2017 study who previously had experienced abuse or harassment online, made changes to the content they share or express online as a result.[54]

3.66 The relative infancy of the technology means it is too soon to draw conclusions about the longer-term impact of witnessing abusive and offensive behaviour online. However, children's charities have shared their concern with us that the impact of regularly seeing widespread abusive and offensive communications online may be particularly pronounced on impressionable members of the community, including children and young people.

IS THE HARM ARISING FROM ONLINE ABUSE DIFFERENT TO THE HARM ARISING FROM OFFLINE ABUSE?

3.67 Many of the harms suffered by victims of online abuse – particularly the general psychological and physiological symptoms – are also harms reported by victims of offline abuse. Some commentators have suggested that online abusive and offensive communication is the same offence both online and offline, just committed in a different format. Analogous themes are explored in the work of Grabosky, who has argued that although some forms of virtual criminality are new, "a great deal of crime committed with or against computers differs only in terms of the medium".[55]

3.68 Victims have told us that they experience online abuse as something qualitatively different to offline abuse. Often, these examples linked back to the characteristics of online communication that we set out from paragraph 2.155 onwards in Chapter 2. These included the volume of communications, reach and permanency of the message, and perceived anonymity of the offender.

3.69 Comments made to us by stakeholders suggest that there is a significant body of opinion that the harm generated by online abuse is not unique. In fact, many people believe that the harms from online abusive and offensive behaviour are overall less serious than the harms stemming from offline equivalents, because the perpetrator is not physically in the same place as the victim and there is often no imminent risk of physical harm.

---

53 A Lenhart and others, *Online Harassment, Digital Abuse and Cyberstalking in America* (November 2016) p 55, available at https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf.

54 A Dhrodia, *Unsocial Media: The Real Toll of Online Abuse Against Women* (20 November 2017), available at https://medium.com/amnesty-insights/unsocial-media-the-real-toll-of-online-abuse-against-women-37134ddab3f4.

55 PN Grabosky, "Virtual criminality: Old wine in new bottles?" (2001) 10 *Social & Legal Studies* 243, p 243.

3.70 Those arguments often stem from the notion that the victim is voluntarily choosing to put themselves in harm's way by remaining online and could make different choices. In their work on female victims of online abuse, Lumsden and Morgan observed:

> The message to women using online spaces which is reflected in media reports can be summed up as similar to the age old sexist adage: "if you can't stand the heat, get out of the kitchen". Victims are advised to remember that no crime is intended (ie it is only "banter") and also not to provoke the troll further. These strategies do not address the issue of abuse, misogyny and sexism, but require women to be complicit in the exercise of "symbolic violence".[56]

3.71 This idea that the harms committed online are avoidable (and thus less serious) misunderstands the nature of online communication and is concerning in a number of respects:

(1) It creates a dichotomy between people's offline and online presence which is not the reality for many social media users. As Jurasz and Barker put it, "it fails to take into account the fact that boundaries between 'online' and 'offline' aspects of everyday life are increasingly disappearing in the context of modern societies".[57]

In fact, the pervasive nature of online communications actually means that online abuse is more likely to be a constant harmful presence in the victim's life. As an anti-bullying charity told the Safety Net inquiry, "thirty years ago, home was a safe place, but now there is no escape from the bullying, which creates constant stress and anxiety which is hard to navigate".[58]

(2) As Henry and Powell argue in their work on technology facilitated sexual violence, it means that there is a missed opportunity to create solutions and innovative responses to these offences. They argue for the need to pay "greater attention and detail to the unique harms experienced by victims" saying that "it is crucial to view these not simply as old crimes, but as unique harms that require innovative responses".[59]

(3) It creates an environment in which the harm caused is implicitly excused and accepted. Jane has described the minimisation of the harm from online abuse as

---

56 K Lumsden and H Morgan, "Media framing of trolling and online abuse: silencing strategies, symbolic violence, and victim blaming" (2017*) Feminist Media Studies* 926, p 926.

57 K Barker and O Jurasz, *Submission of Evidence on Online Violence Against Women to the UN Special Rapporteur on Violence against Women, its Causes and Consequences* (2017) p 4, available at http://oro.open.ac.uk/52611/1/Barker%20%26%20Jurasz%20-UN%20Submission%20on%20online%20violence%20against%20women%20%28Nov%202017%29.pdf.

58 Submission of Liam Hackett, CEO of Ditch the Label, in A Chalk MP, The Children's Society and YoungMinds, *Safety Net: Cyberbullying's impact on young people's mental health, Inquiry report* (2018) p 40, available at https://www.childrenssociety.org.uk/sites/default/files/social-media-cyberbullying-inquiry-full-report_0.pdf.

59 N Henry and A Powell, "Embodied Harms: Gender, Shame and Technology-Facilitated Sexual Violence" (2015) 21(6) *Violence Against Women* 758, p 773.

being analogous to the treatment of other areas of harm where the victimisation of women has been downplayed:

> as with rape, domestic violence and workplace sexual harassment in the 1960s, gendered cyber-harassment is frequently trivialized, mocked, regarded as a personal matter and framed as legally intractable because of its "highly personal and idiosyncratic" contexts.[60]

CAN THE CHARACTERISTICS OF ONLINE ABUSE AGGRAVATE THE HARM CAUSED TO VICTIMS?

3.72 In fact, some data suggest that harm suffered online can be aggravated when compared to equivalent harm experienced offline. Raskauskas and Stoltz, for example, compared traditional and "electronic" (such as online and via mobile phones) bullying amongst adolescents. Although they did not have a group of participants which enabled them to make a conclusive comparison, they noted that:

> Electronic bullying may have more impact on youth's emotional development and well-being than traditional bullying because of an even greater power imbalance created by the fact that many victims of electronic bullying may never know the identity of their bully. Another factor that can make electronic bullying more of a threat to psychological health than traditional bullying is its transcendence beyond school grounds and 24-hr availability such that children are not even safe from bullying in their own homes.[61]

3.73 Studies and experiences shared with us, suggest that the harm is particularly likely to be aggravated (a) when the abuse is visual in nature or (b) when it is perpetrated by a group; both circumstances which are disproportionately likely to happen online because of the characteristics of the online space outlined in Chapter 2.

Online offensive or abusive communication accompanied by visual images

3.74 Many of the examples shared with us by stakeholders, suggested that the presence of a visual image online heightened the impact of abusive and offensive behaviour. That theory has been the subject of some academic research. For example, Smith et al reported that even a short duration of being a cyber victim might have severe effects on secondary school pupils, given the potentially wide audience. Their data suggested that picture/video clip bullying and distributing abusive images of the victim widely in the peer group "would have a strong negative impact on the victim, much more than traditional bullying".[62]

---

60 E Jane, *Rape threats and cyberhate? Vote no to the new digital evidence* (21 June 2015) available at https://theconversation.com/rape-threats-and-cyberhate-vote-no-to-the-new-digital-divide-43388.

61 J Raskauskas and AD Stoltz, "Involvement in traditional and electronic bullying among adolescents" (2007) 43(3) *American Psychological Association* 564, p 565.

62 PK Smith and others, "Cyberbullying: Its nature and impact in secondary school pupils" (2008) 49 *Journal of Child Psychology and Psychiatry* 376, p 383. For discussion of other studies examining the effects of visual imagery in cyber bullying see C Langos, "Cyberbullying: The Shades of Harm" (2015) 22(1) *Psychiatry, Psychology and Law* 106.

3.75 These themes also emerge in discussion of non-consensual sharing of intimate images. In such circumstances, the permanency and resonance of the online image means that "the fact that an image has been altered, or is even composed of images taken of different women, does not diminish the potential harm resulting from its dissemination".[63]

3.76 We discuss this in more detail in Chapter 10.

Online offensive or abusive communications perpetrated by a group

3.77 The presence of organised mobs committing online offences has been well documented. As Citron has observed:

> anonymous online groups… attack women, people of color, and members of other traditionally disadvantaged classes. These destructive groups target individuals with defamation, threats of violence, and technology-based attacks that silence victims and concomitantly destroy their privacy.[64]

3.78 Users have described how abuse coming from a group of people can have a heightened impact, due to its unremitting nature. Offences committed by a group of offenders can often achieve a critical mass which would be very difficult for an individual offender to replicate. For example, Stella Creasey MP has spoken in the media about the "persistence and escalation" of abuse from 148 different social media accounts, which targeted her online, when she publicly supported the campaigner Caroline Criado-Perez.[65] In turn, Ms Criado-Perez, who was campaigning for equal representation of women on banknotes, has described the deluge of abuse that she received online. In a 12-hour period, she reported receiving some 50 rape and murder threats every hour.[66]

---

63 C McGlynn and E Rackley, "More than 'Revenge Porn': Image-Based Sexual Abuse and the Reform of Irish Law" (2017) 14 *Irish Probation Journal* 38, p 41.

64 DK Citron, "Cyber Civil Rights" (2009) 89 *Boston University Law Review* 61, p 62.

65 S Creasy MP, *Stella Creasy Twitter troll hell: "I can't get the last year of my life back"* (29 September 2014), available at https://www.telegraph.co.uk/women/womens-life/11127782/Stella-Creasy-Twitter-troll-hell-I-cant-get-the-last-year-of-my-life-back.html.

66 A Philipson, *Woman who campaigned for Jane Austen bank note receives Twitter death threats* (28 July 2013), available at https://www.telegraph.co.uk/technology/10207231/Woman-who-campaigned-for-Jane-Austen-bank-note-receives-Twitter-death-threats.html. One offender was sentenced for 18 weeks' imprisonment after reportedly sending abusive messages to Stella Creasy MP online. See Press Association, *Man found guilty of sending menacing tweets to Labour MP Stella Creasy* (2 September 2014), available at https://www.theguardian.com/politics/2014/sep/02/stella-creasy-rape-threats-a-joke where it is reported that "he retweeted a threatening message to Creasy which read: 'You better watch your back, I'm going to rape you're a**e at 8 pm and put the video all over [the internet]'. Over the next day [he] … sent a barrage of offensive tweets … including: 'Best way to rape a witch, try and drown her first then just when she's gagging for air that's when you enter' … Later that evening he wrote: 'If you can't threaten to rape a celebrity, what is the point in having them?' … He also branded her an 'evil witch' and wrote: 'What's the odds of [Criado] and Creasy snuggling and cuddling under a duvet checking their tweets and cackling like witches (rape me says Caroline)'."

3.79 In one well-documented instance, Jess Phillips MP reported receiving 600 "negative rape threats" of "I would not rape you" in one evening.[67]

3.80 Other users have spoken to us about the impact of receiving repetitive, abusive messages which singly would not have caused them harm. One stakeholder told us that what affected her was "the persistent 'you fucking bitch'":

> Maybe one off it doesn't matter, but when you have 500 coming into your inbox, 500 people saying it, maybe you don't think that.

3.81 Steve Thresher, a journalist, described his observations of online abuse in an Guardian article, saying:

> And avalanches happen easily online … Mobs can form quickly: once one abusive comment is posted, others will often pile in, competing to see who can be the most cruel. This abuse can move across platforms at great speed – from Twitter, to Facebook, to blogposts – and it can be viewed on multiple devices – the desktop at work, the mobile phone at home. To the person targeted, it can feel like the perpetrator is everywhere: at home, in the office, on the bus, in the street.[68]

3.82 Anecdotally, we have heard examples where the psychological effects of online abuse are exacerbated by being the victim of group offending. For example, Short has noted the effect of the public nature of online group offending on victims:[69]

> the impact of online abuse is greater because your victimisation is broadcast for everyone to see. It's often joined by a third party so the crowd or pack is going after you. So, very quickly, it feels as though the whole world is after you. There might be positive tweets, you might have lots of friends on the outside, but if the crowd has turned against you and is after you, it feels like the world wishes you harm.

3.83 One stakeholder echoed this view, telling us that the experience of being targeted by online abuse is exacerbated by knowledge of the fact that the audience is not intervening:

> People [who are abused online] feel shunned by society. It can be compared to being shouted out in a public place and no one responding.

3.84 Citron has made similar observations, detailing how:

---

67 See, eg M Oppenheim, *Labour MP Jess Phillips receives '600 rape threats in one night'* (31 May 2016), available at https://www.independent.co.uk/news/people/labour-mp-jess-phillips-receives-600-rape-threats-in-one-night-a7058041.html.

68 B Gardiner and others, *The dark side of Guardian Comments* (12 April 2016), available at https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments.

69 Quoted by A Dhrodia, *Unsocial Media: The Real Toll of Online Abuse against Women* (November 2017), available at https://medium.com/amnesty-insights/unsocial-media-the-real-toll-of-online-abuse-against-women-37134ddab3f4.

> anonymous online mobs… terrorize victims, destroy reputations, corrode privacy, and impair victims' ability to participate in online and offline society as equals.[70]

3.85 We discuss some examples of this type of offending behaviour in Chapter 8.

CONCLUSION

3.86 In this Chapter, we have explored the diverse ranges of harms arising from online abuse and asked whether there are distinctions from the harms arising from offline abuse. Although, as we acknowledge, there are no existing measures which allow for a categorical comparison of relative harm, it is clear that there are characteristics of online abuse which may mean that a victim may be subject to more, and aggravated, forms of harm from online offending in some circumstances.

3.87 In the Chapters which follow, we examine the extent to which the current law deals with the possible harm caused to victims online and offline.

[70] DK Citron, "Cyber Civil Rights" (2009) 89 *Boston University Law Review* 61, p 64.

Chapter 4: Communications offences: an overview

INTRODUCTION

4.1 As noted in Chapter 1,[1] this Report is considering eight different types of behaviour that can be criminal. These are: gross offensiveness, obscenity and indecency, threats, harassment and stalking, hate crime, breaches of privacy, false communication, and encouragement of criminal offending.

4.2 In the following chapters we will illustrate how these forms of behaviour can engage a huge range of statutory and common law crimes. There are two broad offences which are often engaged: section 127 of the Communications Act 2003 ("CA 2003") and section 1 of the Malicious Communications Act 1988 ("MCA 1988").

4.3 The purpose of this chapter is to outline the elements of these offences, and to provide the basis for analysis of them in each of the following chapters.

4.4 Below, we analyse section 1 of the MCA 1988 and section 127 of the CA 2003 in turn and provide some background information about the offences and statistics concerning current rates of reporting, prosecution and conviction. We then outline the elements of these offences and note some of their limitations when committed online, as well as the overlaps that exist between them. In the final section, we consider the purpose behind the offences, and whether the reasons for having two sets of separate but overlapping communication offences continue to be satisfactory and defensible.

MALICIOUS COMMUNICATIONS ACT 1988

4.5 Section 1 of the MCA 1988 provides that:

> (1) Any person who sends to another person –
>
> (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 or electronic communication which is, in whole or part, of an indecent or grossly offensive nature;
>
> is guilty of an offence if his purpose, or one of his purposes, in sending it is that it should, so far as falling within paragraph (a) or (b) above, cause distress or

[1] See paragraph 1.29 of this Report.

anxiety to the recipient or to any other person to whom he intends that or its contents or nature should be communicated.

4.6 Originally sections 1(1)(a) and 1(1)(b) did not refer to electronic communications, but this extension was added by section 43(1) of the Criminal Justice and Police Act 2001 and arose from a government strategy document concerning animal rights extremism.[2]

4.7 There are no reliable figures that distinguish the number of charges under section 1 of the MCA 1988 for conduct which is committed wholly or partly online. However, according to internal case management data provided by the Crown Prosecution Service ("CPS"), there were 3058 section 1 charges which reached a first hearing at a magistrates' court in 2017, a considerable increase from previous years.[3] In 2015, the same figure stood at 1955, which grew to 2470 in 2016. There has therefore been an almost 36% increase in the number of section 1 charges brought between 2015 and 2017, and the figures from 2018 already suggest that this increased charging of section 1 is continuing.[4]

4.8 The majority of these charges related to section 1(1)(a) of the MCA 1988.[5]

4.9 As originally enacted, section 1 was a summary only offence punishable by a fine. However, this has recently been amended and section 1 is now an either-way offence.[6] When tried on indictment, a person can now face imprisonment for a term not exceeding two years, or a fine, or both.[7]

Background

4.10 Section 1 of the MCA 1988 was introduced by a Private Member's Bill following recommendations by the Law Commission in our report on "Poison Pen Letters" in 1985.

---

2 "Animal Rights Extremism: Government Strategy – A consultation document" (March 2001), available at http://www.fraw.org.uk/library/direct_action/home_office_2001.pdf. It was proposed "to amend [the Malicious Communications Act 1988] to ensure the defence provided is an objective one, based on reasonable grounds; *to ensure that it covers all forms of communications including electronic mail;* and to mark the seriousness of behaviour of this kind by making it an imprisonable offence for the first time" (emphasis added). See further *Hansard* (HL), 02 April 2001, vol 624, col 687.

3 Note that the CPS does not collect data that constitutes official statistics as defined in the Statistics and Registration Service Act 2007. These data have been drawn from the CPS's administrative IT system, which (as with any large scale recording system) is subject to possible errors with data entry and processing.

4 There were 1688 charges under section 1 of the Malicious Communications Act 1988 which reached a first hearing between January and June 2018.

5 Section 1(1)(a) of the Malicious Communications Act 1988 was charged and reached a first hearing 1654 times in 2015, 2069 times in 2016, and 2623 times in 2017. Section 1(1)(b) of the Malicious Communications Act 1988 was charged and reached a first hearing 301 times in 2015, 401 times in 2016, and 435 times in 2017.

6 Section 32(1) of the Criminal Justice and Courts Act 2015 amended and substituted section 1(4) of the Malicious Communications Act 1988.

7 Malicious Communications Act 1988, s 1(4).

4.11 This 1985 report arose from a review of the (then) common law offence of criminal libel,[8] and identified a gap in the law when "poison pen" letters and similar material were sent, but where the content was not defamatory. We recommended the creation of a statutory offence, the main elements of which became section 1 of the MCA 1988.[9]

4.12 The offence which we recommended extended beyond the sending of poison pen "letters". It was also intended to apply to any "articles" (such as photographs, film, tape or recorded sound) which could convey proscribed messages, as well as articles (such as human excrement) which could be indecent or grossly offensive in themselves, irrespective of any message conveyed with them.

4.13 We presciently noted that "[i]n the not-too-distant future methods of electronic communication are likely to become common in which no article is ever conveyed from the sender to the recipient".[10] Nevertheless, it is of note that we specifically recommended that the new statutory offence should not extend to electronic communications. This was following analysis of extant offences, such as section 43(1) of the Telecommunications Act 1984, the precursor to section 127 of the CA 2003.[11] We noted the breadth of these offences (as they had been interpreted at that time) as they did not require proof of a fault element. The potential ramifications were that this offence extended beyond communications sent by means of a public telecommunications system. We noted that "any possible amalgamation of the two offences would produce a very cumbersome offence which would inevitably have to be broken down into separate components".[12]

4.14 As noted above at paragraph 4.6, however, the offence under section 1 of the MCA 1988 was subsequently amended to include electronic communications. This has created an overlap with aspects of the offences now contained in section 127 of the CA 2003.

The elements which cover conduct and circumstances in section 1 of the MCA 1988

4.15 These elements in section 1 of the MCA 1988 are committed where the following is "sent" to "another person":

(1) a letter, electronic communication or article of any description which either conveys an indecent or grossly offensive message, a threat, or information which is false (the offences in section 1(1)(a)),

---

8 This was abolished by the Coroners and Justice Act 2009, s 73.

9 We recommended that the offence would penalise anyone who "without reasonable excuse, sends or delivers to another person an article which –

(a) is, in whole or in part, of an indecent or grossly offensive nature; or

(b) conveys a message of that nature, or an unwarranted threat, or false information,

if the sender's purpose is that the article should cause the person to whom he sends it distress or anxiety".

10 Poison Pen Letters (1985) Law Com No 147, para 3.5.

11 This was repealed by schedule 19 of the Communications Act 2003 and replaced with section 127 of the Communications Act 2003.

12 Poison Pen Letters (1985) Law Com No 147, para 4.54.

or

(2) an article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature (the offences in section 1(1)(b)).

4.16 The essential features of these elements will be explained below.

"Sends"

4.17 We specifically recommended an offence that was not dependent on receipt of any communication and would be complete upon "sending", and thus a conduct crime.[13] The importance of that approach was reiterated during parliamentary debates.[14] We also recommended that the offence could be committed through sending by any means, rather than limited to a particular medium, such as postal offences.

4.18 Section 1(3), as amended, now clarifies that "sending" includes "delivering or transmitting and to causing to be sent, delivered or transmitted".

4.19 This is a broad formulation that is unlikely to generate problems in the context of electronic communications. For example, even if a message (such as an email message) is sent but fails to get "delivered" to the recipient's mailbox due to a technical error or filtering software, it will still have been "sent".

4.20 Causing a message to be sent, such as by tricking another (innocent) person into sending an electronic communication, is also "sending" within the meaning of section 1(3) for the purposes of the offence.[15]

4.21 Since the offence is now one that can be tried either way, the law of attempts applies in relation to the offence. Under the Criminal Attempts Act 1981, if the defendant intentionally does acts more than merely preparatory to the sending of a message of the type that is proscribed in the section, the defendant is guilty, provided the defendant does so with the relevant intention to cause distress. Therefore, on a literal application, when the defendant types the obscene email with intent to send it to the victim later and to cause distress when it is sent, the defendant could already be guilty of the offence.

"To another person"

4.22 The offence as we originally envisaged,[16] and as enacted, required that the sending was to another "person".[17] This is also clear from the fault element of the offence, which

---

13 Poison Pen Letters (1985) Law Com No 147, para 4.4.

14 Then Minister of State for the Home Office, John Patten MP, noted "[w]e are seeking to get at the malice involved in sending the article, not to measure the success in causing distress by the sender." See *Hansard* (HC),12 February 1988, vol 127, col 624. He later emphasised that "it does not matter whether any distress is caused": *Hansard* (HC) 12 February 1988, vol 127, col 632.

15 Section 127 of the Communications Act 2003 also provides that the offence can be committed by "causing" messages to be sent.

16 Poison Pen Letters (1985) Law Com No 147, para 4.1.

17 Parliamentary debates also reveal that the clear intention for the offences in the Malicious Communications Act 1988 was for the protection of individuals from receipt of malicious communications. The Bill's sponsor, Andy Stewart MP, introduced it by stating "its purpose is to protect individuals from great distress and

requires an intention to cause distress or anxiety to the "recipient"; there must be a recipient in the mind of the sender for the offence to be committed.[18]

4.23 Therefore, if a person, "D", sends another person, "V", an email of the proscribed character and with the relevant fault element, the offence will be committed. The electronic communication will be sent to V, through email systems and an account used by V. The same is true of SMS (Short Message Service) text messages which are sent over mobile phone networks, and social media messages (such as WhatsApp, iMessage and Facebook Messenger) which are sent over various internet protocols.

4.24 The offence has been amended and widened to embrace electronic communications. However, its scope may still be relatively narrow in the online context, due to this limitation, which requires that the electronic communication is sent to "another person".

4.25 Many electronic communications in the online environment will not have a targeted recipient in this way. For example, if someone writes a story and publishes it on their personal website, this would not involve sending it directly to another "person". The electronic communication, containing the content of the story, will be sent to another computer server, which may or may not be accessed by another "person". Even if the story was about another person, that person would only read it if, for example, they became aware of the web address/URI,[19] and used a web browser to access the content of the post.

4.26 This precise issue arose recently in an unreported Crown Court case.[20] The defendant was initially convicted at Furness and District Magistrates' Court for sending another person an electronic communication conveying false information contrary to section 1(1)(a) of the MCA 1988. The information was published on an online blog post and involved serious allegations against a care worker.[21] The defendant appealed his conviction to Preston Crown Court, but his appeal was dismissed. The Criminal Cases Review Commission referred the case back to the Crown Court under section 11(1)(a) of the Criminal Appeal Act 1995, due to uncertainty in relation to the words "sends to another person" and whether it rightly applied to the defendant's blog post.

4.27 On referral back to Preston Crown Court, the appeal against conviction was allowed and the conviction was quashed. The Court found that the blog post was not sent to

---

anxiety". *Hansard* (HC), 12 February 1988, vol 127, col 607. This was repeated by a number of other MPs supporting the Bill.

18 If a person sends an electronic communication to a computer server, such as by uploading a document to a private online file storage facility for their own use only, the offence will not be committed. There are two possible "recipients" in this example. First, the sender themselves could be viewed as a recipient, as they may subsequently access the document. However, there is no offence under section 1 of the Malicious Communications Act 1988, as it will not have been sent by a person to "another person". Secondly, even if the computer server(s), or the company hosting the content, is viewed as a "recipient", it is not a "person" and it would be nonsensical to say that someone could intend a computer server or company distress or anxiety.

19 URI: Uniform Resource Identifier.

20 *Michael John Paley* (2018) Preston Crown Court (unreported), HHJ Brown.

21 See further *Man accused of sexually abusing his own mum wins six-year battle for justice* (1 May 2018), available at http://www.nwemail.co.uk/news/millom/16425863.man-accused-of-sexually-abusing-his-own-mum-wins-six-year-battle-for-justice/.

"another person" even if it was about another person, regardless of whether the appellant intended the person to read it. The Court noted that this did not mean that the law was incapable of dealing with such behaviour. According to HHJ Brown (the Hon Recorder of Preston) the correct charge was under section 127(2)(a) or 127(1)(a) of the CA 2003. We discuss these offences further below from paragraph 4.52.

4.28 An interpretation based on our 1985 paper and the drafting intention of the section 1 offence supports this conclusion. However, this does limit the scope of the offence considerably, and would cause practical difficulties where section 1 of the MCA 1988 is charged.

4.29 For example, if a person sends a grossly offensive and publicly accessible "tweet", which appears on the Twitter feeds of those that "follow" the person on the platform, it is unclear, following the *Paley* decision, if all followers would be considered persons to whom the "tweet" was sent. Alternatively, the tweet may lack a targeted recipient, because of the generic nature of the electronic communication.[22] However, even if such an act falls outside the remit of section 1 of the MCA 1988, it may be prosecuted as sending a grossly offensive message via a public electronic communications network under section 127(1) of the CA 2003 (see paragraph 4.52 below).

4.30 Interpretative challenges such as this are likely to continue to emerge in circumstances where section 1 is charged in the online context, and where the communication is not targeted at a specific person.

Scope of matter sent

4.31 The offence in section 1(1)(a) of the MCA 1988 applies broadly to any letter, electronic communication or article (of any description) which conveys a message which is indecent or grossly offensive, a threat, or information which is false.

4.32 In the online environment, the offence will often be committed by sending electronic communications with words of the proscribed character, but it could also clearly be committed by sending images, drawings, video or sound recordings or such like.[23]

4.33 Section 1(1)(b), on the other hand, applies to the sending of any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature.

4.34 This offence was intended to cover situations where the article itself, rather than any message or information contained in the communication, was of the proscribed character. For example, if someone sends to another human excrement it could be argued that it does not convey any proscribed message, but rather it is grossly offensive in itself.[24] A very recent such case was *Miah v CPS*[25] where a man pleaded guilty to an

---

22 On the other hand, where specific individuals are "tagged" in the tweet through inclusion of their Twitter handles in the message, this would quite clearly appear to be within the scope of the offence.

23 In our 1985 report, we intended the offence to apply in this broad manner, though not by sending electronic communications as will be discussed below. See Poison Pen Letters (1985) Law Com No 147, para 4.8.

24 Poison Pen Letters (1985) Law Com No 147, para 3.3.

25 (23 October 2018) DC (unreported).

offence contrary to section 1(1)(b) of the MCA 1988 after sending soiled toilet paper to two victims.

4.35 In the online context, if someone sends to another person an electronic communication with an image which is indecent or grossly offensive, it might not convey any message for the purposes of section 1(1)(a) of the MCA 1988. Nevertheless, it could still fall under section 1(1)(b) as it is an electronic communication that is, in part, of an indecent and/or grossly offensive nature.

Electronic communication

4.36 The meaning of an electronic communication is further defined in section 1(2A) and includes "(a) any oral or other communication by means of an electronic communications network and (b) any communication (however sent) that is in electronic form".

4.37 The term "electronic communications network" was inserted by the CA 2003,[26] and is defined by section 32(1) of that Act.[27] The key aspect of the definition is that it provides for the offence to cover a "transmission system" – and associated equipment and software etc – used to convey electronic signals. For example, this would include wired and wireless networks, such as a mobile phone network.

4.38 Any communications sent over the internet – such as email or social media messages – will be sent by means of electronic communications networks. Voice or video calls facilitated by internet protocols (such as the Skype protocol), will similarly come within the meaning of an electronic communication in section 1(2A)(a) of the MCA 1988.

4.39 Section 1(2A)(b) of the MCA 1988 ensures that even where electronic communications are sent otherwise than by means of electronic communications networks, they may still come within the section 1 offence. For example, Bluetooth data exchanges might be regarded as not being sent by means of electronic communications networks,[28] or at least not "public" electronic communications networks, which is a requirement for the offence in section 127. In such cases, the lacuna may be filled by section 1 of the MCA 1988, provided the fault element can be proved. There will still be an electronic communication within the meaning of section 1(2A)(b), as it is a communication "that is in electronic form".

---

26 Communications Act 2003, Sch 17, para 90.

27 "Electronic communications network" means "(a) a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description; and (b) such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals – (i) apparatus comprised in the system; (ii) apparatus used for the switching or routing of the signals (iii) software and stored data and (iv) (except for the purposes of sections 125 to 127) other resources, including network elements which are not active".

28 Personal area networks utilising Bluetooth technology could possibly be found to be a transmission system and thus fall within the definition of an electronic communications network, but this would depend on the underlying technology and the interpretation of section 32(1) of the Communications Act 2003.

The fault element

4.40 A person will only commit an offence under section 1(1) of the MCA 1988 if their purpose, or one of their purposes, in sending the article, letter or electronic communication is to cause distress or anxiety to the recipient or to any other person to whom they intend that it or its contents are communicated. It is worth reiterating that distress or anxiety does not need to be caused to victims; it must only be a purpose in sending the communication.

4.41 The creation of the offence in this model – based on conduct of the defendant rather than proof of harm to a victim – was specifically to address cases where the defendant argued that the purpose or motivation behind their sending was legitimate and not primarily to cause distress or anxiety.[29]

4.42 This issue arose squarely in the case of *Connolly v DPP*. In this case, the defendant sent pictures of an aborted foetus to three pharmacists, and she was charged under section 1 of the MCA 1988.[30] She argued that her purpose "was not to cause distress or anxiety but merely to make a lawful protest and educate against the use of the 'morning after pill'".[31]

4.43 Dyson LJ, delivering the judgment of the Court, found that the trial court was entitled to find on the facts that the photographs were sent for the purpose of causing distress or anxiety,[32] even if they were also sent for a political or educational purpose.[33]

4.44 While there may be difficulties in proving the fault element in such cases, Dyson LJ also opined that the "nature of the communication may shed light on the defendant's mens rea [or fault element]".[34]

4.45 The test is therefore one based on proof of purpose or purposes, and it will only be satisfied where D acts in order to bring about a particular consequence. If, as the trial court found, Connolly had set out both to educate and to cause distress, they were her purposes. On appeal, the trial court's finding that the photographs were sent for the purpose of causing distress or anxiety was not challenged.[35] It may have been arguable that she had set out to bring about education and did not have distress as a purpose; it was one of her oblique intentions. If a consequence is not sought (here distress or anxiety to the recipient), even though it is foreseen as a virtually certain consequence,[36] it is not clear that the mens rea of the offence is satisfied, given the purposive nature of the mens rea in section 1 of the MCA 1988.

---

29 Poison Pen Letters (1985) Law Com No 147, para 4.32. We had specifically recommended that "it should be sufficient that among the defendant's purposes is the purpose of causing distress or anxiety to the person to whom the article is sent" (para 4.35).

30 *Connolly v DPP* [2007] EWHC 237 (Admin); [2008] 1 WLR 276 at [3].

31 *Connolly v DPP* [2007] EWHC 237 (Admin); [2008] 1 WLR 276 at [4].

32 *Connolly v DPP* [2007] EWHC 237 (Admin); [2008] 1 WLR 276 at [11].

33 *Connolly v DPP* [2007] EWHC 237 (Admin); [2008] 1 WLR 276 at [9].

34 *Connolly v DPP* [2007] EWHC 237 (Admin); [2008] 1 WLR 276 at [9].

35 *Connolly v DPP* [2007] EWHC 237 (Admin); [2008] 1 WLR 276 at [11].

36 *R v MD* [2004] EWCA Crim 1391.

4.46 Where section 1 is charged in the context of sending false information, the sender will only be liable where it is known or believed to be false. We discuss this further in Chapter 11.

Defences

4.47 Many communications sent for a legitimate purpose may actually satisfy the elements in the offence under section 1 of the MCA 1988. For example, a debt collector who sends an email threatening recovery action is sending an electronic communication to another person which conveys a threat. If he intends to send the email to the other person, and one of the purposes for sending it is to cause distress or anxiety to the recipient, then the offence is complete.

4.48 In our 1985 recommendations for the offence under section 1 of the MCA 1988, we addressed this issue by recommending that the offence be only committed where a threat is "unwarranted".[37]

4.49 Our formulation was adapted from section 21 of the Theft Act 1968,[38] but the recommendation that the burden of proof should be the same as section 21 was not adopted in the MCA 1988.[39]

4.50 Section 1(2) now makes provision for certain legitimate threats, and clarifies the circumstances when an offence is not committed by virtue of section 1(a)(ii) of the MCA 1988. A person is not guilty of this offence if "he shows that the threat was used to reinforce a demand made by him on reasonable grounds; and that he believed, and has reasonable grounds for believing, that the use of the threat was a proper means of reinforcing the demand".[40]

4.51 Therefore, even where a defendant sends a message and one of the defendant's purposes is to cause anxiety by the threat (for example, of legal action if payment is not made for services rendered and contractually agreed), the defendant may not have

---

37 Poison Pen Letters (1985) Law Com No 147, paras 4.36 to 4.41. In the recommendations for a new statutory offence, we defined the circumstances when a threat would be warranted. This was "only if the person sending or delivering the article in question uses the threat to reinforce a demand which he believes he has reasonable grounds for making, and he believes the use of this threat to be a proper means of reinforcing the demand" (para 5.4).

38 Poison Pen Letters (1985) Law Com No 147, para 4.40.

39 Poison Pen Letters (1985) Law Com No 147, para 4.41. We recommended the "burden of proof here would not differ from that under the proviso to section 21 of the Theft Act 1968: if the evidence raises the issues contained in either paragraph of clause 1(2), the prosecution must negative them beyond reasonable doubt". When the Malicious Communications Bill was introduced, however, Andy Stewart MP (presenting the Bill) explained that it "specifically requires that the defendant must prove that he had reasonable grounds for making such an accusation". *Hansard* (HC), 12 February 1988, vol 127, col 607. The Minister of State for the Home Office also noted six points of "dissent" from the Law Commission's recommendations, one of which was that "the burden of proof that a threat was warranted should be transferred from the prosecution to the defence". *Hansard* (HC), 12 February 1988, vol 127, col 635. Use of the word "shows", rather than "proves" was challenged during parliamentary debates but the former was nevertheless adopted, see *Hansard* (HC), 12 February 1988, vol 127, col 651 to 652.

40 Malicious Communications Act 1988, s 1(2). Prior to 2001, the test was a subjective one, but it was amended to become an objective test of reasonableness by section 43 of the Criminal Justice and Police Act 2001.

committed the offence.[41] The threat could have been made to reinforce a demand for payment and on reasonable grounds, and the defendant may believe, and have reasonable grounds for believing, that this was a proper means of reinforcing the demand. Such cases will turn on the context and this objective assessment of what the defendant subjectively believed. If the threat of legal action was highly abusive, the defendant may not have reasonable grounds for believing that this was a "proper" means of reinforcing the demand.

SECTION 127 OF THE COMMUNICATIONS ACT 2003

4.52 Section 127 of the CA 2003 provides as follows:

> (1) A person is guilty of an offence if he—
>
> (a) sends 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.
>
> (2) A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he—
>
> (a) sends by means of a public electronic communications network, a message that he knows to be false,
>
> (b) causes such a message to be sent; or
>
> (c) persistently makes use of a public electronic communications network.

4.53 Like section 1 of the MCA 1988, offences under section 127(1) and (2) are frequently prosecuted, particularly in the context of social media communications.

4.54 According to internal management data provided by the CPS, there were 2963 section 127 offences charged and reaching a first hearing at a magistrates' court in 2017. This is a slight increase from previous years (2957 in 2016, and 2796 in 2015).[42]

4.55 The majority of these charges related to section 127(1) offences,[43] though the charging of offences in section 127(2) is not uncommon. Section 127(2)(c) was charged 437

---

41 Examples like this were considered during the parliamentary debates. See *Hansard* (HC), 12 February 1988, vol 127, col 633.

42 As noted previously in this Chapter, the CPS does not collect data that constitutes official statistics as defined in the Statistics and Registration Service Act 2007. These data have been drawn from the CPS's administrative IT system, which (as with any large scale recording system) is subject to possible errors with data entry and processing.

43 Section 127(1) of the Communications Act 2003 was charged and reached first hearing 1936 times in 2015, 2210 times in 2016, and 2272 times in 2017.

times in 2017, while there were 254 charges under section 127(2)(a) and (b) in the same year.[44]

4.56 The offences can only be tried in the magistrates' court. The penalty for an offence under section 127 is six months' imprisonment, or a fine, or both. The Magistrates' Court Sentencing Guidelines were revised in 2017, and now detail the forms of culpability and harm which will warrant periods of imprisonment for section 127 offences.[45]

Background

4.57 The offences contained in section 127 of the CA 2003 can be traced to legislation relating to the misuse of public service facilities, such as the postal service,[46] and British Telecom when nationalised.

4.58 Section 10(2) of the Post Office (Amendment) Act 1935 made it an offence where a person:

(a) sends any message by telephone which is grossly offensive or of an indecent, obscene, or menacing character; or

(b) sends any message by telephone, or any telegram, which he knows to be false, for the purpose of causing annoyance, inconvenience, or needless anxiety to any other person; or

(c) persistently makes telephone calls without reasonable cause and for any such purpose as aforesaid.

4.59 These offences were broadly replicated in subsequent legislation: section 66(a) of the Post Office Act 1953; section 78 of the Post Office Act 1969; section 49(1)(a) of the British Telecommunications Act 1981, and section 43(1)(a) of the Telecommunications Act 1984.[47]

4.60 It is striking that the offences in section 127 of the CA 2003 are almost a word-for-word repetition of the 1935 offences, save that the proscribed messages or matters sent are now criminalised where sent over a public electronic communications network, which is discussed below at paragraphs 4.83 to 4.93.

---

44 The figures from 2016 were 268 charges under section 127(2)(a) and (b) and 479 charges under section 127(2)(c). This was a decrease from 2015: 322 charges under section 127(2)(a) and (b) and 538 charges under section 127(2)(c).

45 See: Sentencing Council, *Communication network offences* (2017), available at https://www.sentencingcouncil.org.uk/offences/item/communication-network-offences-revised-2017/.

46 Section 4(1)(c) of the Post Office (Protection) Act 1884 prohibited sending packets that contained any words, marks or designs of an indecent, obscene, or grossly offensive character.

47 For a full outline of the historical changes which occurred across these provisions see *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [6]. Section 11 of the Post Office Act 1953 also criminalised the sending of indecent or obscene material through the post. These offences are now contained in section 85(3) and (4) of the Postal Service Act 2000.

4.61 The purpose of the offences under section 10(2) has previously been described as being originally aimed at protecting telephone operators.[48] However, the legislative background to the offences actually reveals that the drafters specifically intended them to protect members of the public more broadly.[49]

4.62 Today, section 127 of the CA 2003 applies to communications sent over services such as Twitter and Facebook that were not even in existence when the CA 2003 was enacted.

4.63 The result is that we now have a set of offences that are remarkably broad, both in terms of the different forms of communications now captured, and the proscribed behaviour and speech caught by the section 127 provision. When combined, the result is a criminalisation of some forms of communication that many may find surprising. Lord Brown, for example, has raised the question of whether use of telephone (sex) chat-lines constitutes a criminal offence under section 127, as the essence of these conversations will entail sending indecent or obscene messages.[50] Indeed, as subsequent Chapters will illustrate, section 127 of the CA 2003 criminalises many forms of speech that would not be an offence in the "offline" world, even if spoken with the intention described in section 127.[51]

The elements which cover conduct and circumstances in section 127 of the CA 2003

4.64 The external elements of the offences in section 127(1) consist of:

(1) sending a message or other matter;

(2) of the proscribed character;

---

48 Lord Judge CJ has suggested that the offences originally had a narrow focus: "… because of the limited technology available at the time, these messages would largely be communicated to a single, often deliberately targeted recipient like telephone operators, who were subjected to indecent, obscene or menacing messages": *Chambers v DPP* [2012] EWHC 2157, [2013] 1 WLR 1833 at [27]. See also the remarks of Sir Keir Starmer QC while DPP: "it is perhaps worth remembering that the Communications Act was originally drafted in 1935, to protect telephone operator staff from abuse. Through various re-enactments its reach has extended from telephones to all those using the internet": K Starmer, *Social Media Prosecutions: Why I Have Published Guidelines Today* (19 December 2012, updated 18 February 2013), available at https://www.huffingtonpost.co.uk/keir-starmer-qc/twitter-laws-social-mediaprosecutions_b_2328248.html.

49 See *Hansard* (HL), 19 March 1935, vol 96, col 163 to 164. Having spoken of the protection afforded to telephone operators, Lord Templemore noted: "during the debate on the Second Reading in the House of Commons *it was suggested that the public should also be protected and subsection (2) has been designed accordingly.* In its three paragraphs protection is afforded not only against the improper use of the telephone but also the telegram. Cases have occurred where members of the public have received over the telephone messages of an indecent character, and even of a menacing character. There have also been instances where telegrams have been sent to persons intimating that somebody is seriously ill and when inquiries have been made by anxious friends or relatives the message has been found to be a complete hoax. There have also been cases of annoyance caused by persons who persistently use the telephone to make calls without reasonable cause – usually late at night. *This subsection will give the Postmaster-General the necessary power to protect the public"* (emphasis added).

50 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [27].

51 Though the broad terms of the offence of harassment, alarm or distress under section 5 of the Public Order Act 1986 – which is primarily designed for the offline context, does overlap to a significant degree.

(3) by the defined means.

4.65 The first element will ordinarily be satisfied by the sending of a "message". Unlike the offence under section 1 of the MCA 1988, which, as examined above, can also be committed by sending physical articles like human excrement, the offences in section 127 can only ever be committed by the sending of data by the defined means. As a noun, the term "message" could be broad enough to cover both the data making up the communication itself (for example, a social media "instant message" or email as an electronic mail "message") as well as information that is conveyed through it. A communication could, for example, only be of the proscribed character owing to the information that can be gleaned from it in a particular context.

4.66 The term "other matter" serves as a "catch-all" expression, but since "message" can be interpreted broadly in the context of electronic communications, prosecutions for the sending of "other matter" are likely to be rare. Telephone calls, emails, website publications, social media postings will all involve the sending of "messages."

4.67 The offences in section 127(2)(a) and (b) of the CA 2003 are only committed by sending "messages".

4.68 The proscribed character refers to messages that are "grossly offensive", "indecent", "obscene", or "menacing".

4.69 The "defined means" is that the message or other matter is sent by means of a public electronic communications network. This is explained at paragraph 4.37 above.

4.70 One issue that is not clear on the face of section 127(1) is whether the message or other matter must have been received or read by another person for the offence to have been committed. This issue has been judicially clarified.

4.71 It was confirmed by the House of Lords in *DPP v Collins* that the section 127(1) offences are conduct crimes. Lord Bingham – with whom the other members of the Court agreed – noted that "[t]he offence is complete when the message is sent".[52]

4.72 Like section 1 of the MCA 1988, this means that it does not matter whether anyone reads or even receives the message. If a person sends a proscribed message using a social media service and later regrets their actions and deletes the message before it is read by another, the offence will still have been committed.

4.73 This also means that liability will not turn on how the message was received or understood by recipients. Those that read them may not even find the messages indecent or offensive, but if they are deemed to be of the proscribed character as a question of fact, then this element of the offence will be complete.[53]

---

[52] *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [7].

[53] *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [9].

4.74 The courts will, however, take into account all relevant circumstances when determining whether messages are of the proscribed character, and the impact on the recipient can be considered for this purpose.[54]

4.75 In the context of menacing messages, the High Court has said that "a message which does not create fear or apprehension in those to whom it is communicated, or who may reasonably be expected to see it, falls outside this provision, for the very simple reason that the message lacks menace".[55]

4.76 This has caused some confusion as to whether the section 127(1) offence is a result crime or a conduct crime where the "menacing" variant of the offence is charged.[56] However, the better reading of both *Collins*[57] and *Chambers v DPP*[58] is that receipt is not required. If a person reading the message would feel fear or apprehension, then the conduct element of the offence is complete upon sending. In the context of sending menacing messages, "the effect of the message on those who read it is not excluded from the consideration",[59] but receipt and reading is not a prerequisite. This was more recently confirmed by the High Court in the context of both grossly offensive and menacing messages, and the same must also be true of obscene and indecent communications.[60]

4.77 Therefore, unlike section 1 of the MCA 1988, a person can, strictly speaking, commit the offence in section 127(1) even if they only intend to store communications for themselves using online storage facilities. Judges, when outlining the fault element of the offence, often envisage a recipient, or at least the possibility that the communications may be accessed by members of the public. However, this possibility of access by others does not appear necessary for the offence to be committed. As will be discussed below at paragraphs 4.83 to 4.93, the offence in section 127 is purportedly aimed at ensuring propriety in communications over public electronic communications networks.[61] This also suggests that the offence is not exclusively concerned with protecting other people from receipt of unsolicited messages of the proscribed

---

54 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [9].

55 *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [30].

56 A Gillespie, *Cybercrime: Key Issues and Debates* (2016), p 264. This aspect of the *Chambers* decision was also slightly misstated in *Karsten v Wood Green Crown Court* [2014] EWHC 2900 at [17] where it was suggested that this variant of the section 127(1) offence was a result crime and will only be committed where the message creates "a sense of apprehension or fear in the person who receives or reads it".

57 [2006] UKHL 40; [2006] 1 WLR 2223.

58 [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833.

59 *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [32].

60 See *DPP v Smith* [2017] EWHC 359 (Admin) at [28] and [33], where Sweeney J accepted a submission that the "the actus reus is complete at the time of the sending. It makes no difference whether the relevant message is received or read or not, or who (if anyone) actually receives it". The same submission also made the point that "whilst in *Chambers* the court decided, on the very particular facts of that case, that the application of that objective test does not necessarily exclude from consideration the reaction of, or any effect on, a person who had actually received or read the relevant message, the need for any such consideration was likely to be relatively rare, and the weight attached to it was likely to be relatively limited".

61 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [7].

character.[62] Therefore, if someone takes "obscene" photographs of themselves, or writes an "indecent" fantasy about a sexual experience, and saves these in a private online file storage facility (where there is little possibility of these being seen by others) the offence may still be complete if its fault element is present (we discuss the fault element of the offence further at paragraphs 4.94 to 4.105 below). If the same content was printed or typed, and stored in a drawer in a person's house, no offence would be committed without more. This again raises questions about the scope of the offence, and its compatibility with the rights to privacy and the freedom of expression.

4.78 This example illustrates how an offence that had its roots in the protection of telephone operators and the public, has developed into a much broader offence that may even criminalise sending messages to oneself.

4.79 Section 127(1)(b) and 127(2)(b) capture conduct that may be remote from the actual sending of proscribed messages or other matter. In the context of the proposals that led to section 1 of the MCA 1988, we considered the need to include a causal conduct element (for example, "causes to be sent"). However, we recommended against this, and considered that the term "sends" would be broad enough to embrace scenarios such as where someone asks another to post a letter for them.[63] In both section 1 of the MCA 1988 and section 127 of the CA 2003, this recommendation was not followed, and a causal conduct element was included within most of the section 127 offences (the exception is section 127(2)(c)).

4.80 Therefore, if the defendant dupes another into sending a grossly offensive, obscene, indecent, menacing, or false message, then the defendant could, arguably, be prosecuted for sending the message, but certainly for "causing" such a message to be sent, provided the fault element for these offences is satisfied.[64] Another example may be where someone sends a hyperlink to a website that contains proscribed content within the meaning of section 127. The words and characters making up the hyperlink could be entirely innocent and lawful but the website could contain proscribed messages or other matter. The sender of the hyperlink could argue that they did not actually send the proscribed content and that they only "sent" the letters and characters that made up the hyperlink. Such an argument could succeed in the context of section 127(1)(a) and 127(2)(a), but would be likely to fail if section 127(1)(b) and 127(2)(b) were charged. If the recipient clicks through to the proscribed material from the hyperlink, then the servers hosting the material would send it to the requesting "client".

4.81 There is no specific authority on the question of whether the offences in section 127(2) are conduct crimes, however they are likely to interpreted as such. Like the offences under section 1 of the MCA 1988 (which require that one of the defendant's purposes is to cause "distress or anxiety") the fault element in section 127(2) CA 2003 contains

---

62 This can be contrasted with section 1 of the Malicious Communications Act 1988, which Lord Bingham has said is aimed at "protect[ing] people against receipt of unsolicited messages which they may find seriously objectionable:" See *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [7].

63 Poison Pen Letters (1985) Law Com No 147, para 4.5: "…it is sufficiently clear in the context of the offence which we are recommending that, where one person asks another to put his poison-pen letter in the post-box, he himself "sends" the letter".

64 See also the offences in sections 44 to 46 of the Serious Crime Act 2007 (encouraging or assisting offences) which are discussed in Chapter 12. These are alternative charges in this situation.

an ulterior intent. In this case, it is that the defendant has sent it for the purposes of causing "annoyance, inconvenience, or needless anxiety". However, actual harm does not need to arise as a result of sending the message for the offence to be committed.

4.82 For example, if a person publicly posts a message on a social media website that they know to be false (such as, "the Pope has been assassinated') and they intend by doing so to, for example, cause needless anxiety to another, the offence is committed as soon as the message is sent. There is no need to show that another person received the communication or was caused annoyance, inconvenience, or needless anxiety.

Meaning of "public electronic communications network"

4.83 Section 127 criminalises the sending of proscribed messages or other matter "by means of a public electronic communications network".

4.84 A public electronic communications network is defined in section 151(1) of the CA 2003 and means "an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public."

4.85 The meaning of an "electronic communications network" has been discussed above at paragraph 4.37.

4.86 There has previously been some confusion as to whether messages sent on social media websites and applications like Facebook, Facebook Messenger and Twitter are within the scope of the offences under section 127 of the CA 2003. It was argued in *Chambers,* for example, that messages sent using Twitter were not sent by means of a "public electronic communications network".[65] While "over the top" communications services such as Facebook and Twitter are colloquially referred to as "social networks" and are available to the public, they are not in fact "public electronic communications networks" from a regulatory perspective. Rather, they are "information society services"[66] though somewhat of a hybrid and also sharing features of an "electronic communication service".[67]

4.87 These distinctions did not, however, prevent section 127 from applying. The Crown Court judge in *Chambers* opined that because services like Twitter can only operate through the internet, which consists of public electronic communications networks, then

---

65 *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [21].

66 In the current EU regulatory framework, the term "information society service" is defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services": Article 1(b), Directive 2015/1535.

67 For discussion see N Brown, "An assessment of the proportionality of regulation of 'over the top' communications services under Europe's common regulatory framework for electronic communications networks and services" (2014) 30 *Computer Law and Security Review* 357, pp 359 to 360. A draft Directive that is currently before the European institutions is addressing this overlap between the definitions of "information society services" and "electronic communications services". See Recital 10 of "Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast)", available at https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code.

the messages are sent "by means of" a public communications network.[68] The Divisional Court agreed with this approach. Messages sent over Twitter were found to fall within the ambit of the section 127 offence, despite Twitter not constituting a public electronic communications network itself.[69]

4.88 This means that almost all forms of internet based communications today fall within the scope of the section 127 offence. Use of service providers which facilitate email, messaging or blogging will entail communications sent over the internet in this way.

4.89 There are, however, some forms of communication that are outside the scope of the offence. Messages that are sent in some private or restricted networks (for example, local area networks for a corporate firm) are not made available to members of the public and thus fall outside the definition of a "public" electronic communications network. This is distinct from internet enabled messaging services such as WhatsApp and Facebook Messenger, which do fall within section 127.

4.90 For example:

> D and V work for a company that has its own private local area network. Software allows members of staff to message each other over this network. D sends V, a black woman, a racist message that is undoubtedly grossly offensive.

4.91 In the above example, section 127 could not apply because it is sent over a private electronic communications network. However, if D had used internet networks and services that are made available to the public, he or she would be liable. The conduct of D is arguably the same, but he is saved by the private nature of the network. In fact, D may not even realise that it is a private network. Thus, V's only recourse is to employment law rather than criminal law (unless D's behaviour falls within section 1 of the MCA 1988, but then it would be necessary to prove the intention to cause anxiety or distress).

4.92 Some technologies also enable direct point-to-point communications. "Bluetooth", for example, enables direct communications between mobile phones, which would not be sent "by means of" a public communications network. If someone's device is configured to receive Bluetooth communications, photos or videos could be sent to them directly from another Bluetooth device, but only within a relatively small range. Usually, the maximum range for Bluetooth communications is approximately one hundred metres, though this depends on the Bluetooth version[70] and factors such as the output power of the transmitter and whether there are any physical obstacles.

---

68 *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [23].

69 *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [24] to [25].

70 Bluetooth version 5 has the widest possible range.

4.93 There have been reported incidents of "cyber flashing" where proscribed images are sent via Bluetooth and Apple's Airdrop service.[71] Where this occurs, offences such as section 1 of the MCA 1988 would need to be charged, rather than section 127 of the CA 2003.[72] This will only be possible where the fault element (a purpose to cause distress or anxiety to the recipient) in section 1 is present.

The fault element

4.94 Unlike section 1 of the MCA 1988, section 127(1) of the CA 2003 does not have any express provision for the fault element (mens rea) of the offence.

4.95 In *Collins*, Lord Bingham referred to longstanding authority that where a legislative offence does not contain any explicit fault element, it is the court's duty "to read in words appropriate to require mens rea".[73] Parliament is presumed not to have intended "to make criminals of persons who were in no way blameworthy in what they did".[74]

4.96 Counsel in *Collins* argued that the appropriate fault element for the offence in section 127(1)(a) could be read in by taking the fault element of section 6(4) of the Public Order Act 1986 as a model.[75] This envisages liability where a person either intends his or her words or behaviour to be of the proscribed character, or where he or she is *aware* that they may be so. This is, therefore, a form of subjective recklessness where advertent risk-taking will suffice for a prosecution to succeed.

4.97 The House of Lords agreed with this submission. Beyond requiring an intention to send the message in question,[76] Lord Bingham stated (in the context of grossly offensive messages) that the appropriate fault element for the offence in section 127(1) is:

> 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.[77]

4.98 This was followed in *Chambers* in the context of menacing messages. The offence is committed where:

---

71 See, eg S Bell, *Police investigate "first cyber-flashing" case* (13 August 2015), available at https://www.bbc.co.uk/news/technology-33889225.

72 The underlying wireless technology could be found to be an electronic communications network itself, for the purposes of section 1(2A)(a) of the Malicious Communications Act 1988. This is discussed above at paragraph 4.37. Alternatively, such cyber flashing would certainly constitute a communication in "electronic form" within the meaning of section 1(2A)(b) of the Malicious Communications Act 1988.

73 *Sweet v Parsley* [1970] AC 132 at 148 per Lord Reid (quoted by Lord Bingham in *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [11]).

74 *Sweet v Parsley* [1970] AC 132 at 148 per Lord Reid (quoted by Lord Bingham in *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [11].) See further *B v DPP* [2000] UKHL 1; 2 AC 428 and *R v K* [2001] UKHL 41; [2002] 1 AC 462.

75 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [10].

76 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [10].

77 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [11].

the offender is proved to have intended that the message should be of a menacing character (the most serious form of the offence), or alternatively, if he is proved to have been aware of or to have recognised the risk at the time of sending the message that it may create fear or apprehension in any reasonable member of the public who reads or sees it.[78]

4.99 In *Chambers,* Lord Judge CJ – with whom the other members of the Court agreed – also opined that the same fault element criteria applied in relation to the other classes of behaviour prohibited by section 127(1).[79] This appears to mean that sending obscene or indecent messages or other matter by means of a public electronic communications network will only be an offence if it is intended by the sender that the message or other matter is obscene or indecent, or the sender is aware of the risk that a reasonable member of the public would view it as obscene or indecent.[80] The more recent High Court decision in *Smith* also supports this interpretation of the fault element of the offence.[81]

4.100 Therefore, in contrast to the offences in section 1 of the MCA 1988 and section 127(2) of the CA 2003, the offences in section 127(1) of the CA 2003 are of basic intent.[82]

4.101 Offences under sections 127(2)(a) and (b) will only be committed if the message is:

- knowingly sent (or knowingly caused to be sent in the context of section 127(2)(b));
- known to be false; and
- for the purpose of causing annoyance, inconvenience or needless anxiety.

4.102 The offence in section 127(2)(c) will similarly only be committed if there is an ulterior intent to cause annoyance, inconvenience or needless anxiety.

4.103 Some of these variants are not very demanding as fault element criteria. Anyone who regularly uses the internet in order to "annoy" others could technically commit the

---

78 *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [38].

79 *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [36].

80 *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [36]. The factual differences between *Collins* and *Chambers* meant that the recklessness element was described differently in each case. In *Collins* the offensive messages were targeted at a Member of Parliament and his staff, and Lord Bingham described the fault element in terms of the risk of grossly offending "those to whom the message relates". However, *Chambers* illustrates that the offence in section 127(1) of the Communications Act 2003 can also be committed even where the messages are not targeted at a specific individual, or relate to a specific individual. The "tweet" was a general threat (although found to be a joke) and seemingly accessible to all. This may explain why subjective recklessness was described in the case as being met where the offender is aware of the risk that a reasonable member of the public who reads or sees it may be put in fear or apprehension.

81 Like *Collins,* this case concerned grossly offensive communications, and Sweeney J accepted a submission that the mens rea (fault element) of the offence was where the offender "intended his message to be grossly offensive to those to whom it related; or that he was aware at the time of sending that it might be taken to be so by a reasonable member of the public who read or saw it": see *DPP v Smith* [2017] EWHC 359 (Admin) at [28] and [33].

82 *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [36].

offence in section 127(2)(c). Strictly speaking, this could, for example, cover a politician or political commentator who regularly posts social media messages in order to annoy others – perhaps those with whom they disagree politically. The implications for the freedom of expression would be particularly acute if the offences were prosecuted and enforced in this way.

4.104 The *Chambers* case also illustrates how difficult it can be to establish the fault element of these offences without information about the context behind communications. Lord Judge CJ emphasised that:

> the [fault] element of the offence is directed exclusively to the state of mind of the offender, and that if he [Chambers] may have intended the message as a joke, even if a poor joke in bad taste, it is unlikely that the [fault element] required before conviction for the offence of sending a message of a menacing character will be established.[83]

4.105 Distinguishing between good jokes, bad jokes, and illegal jokes can be an unenviable task for law enforcement, particularly where there is also a lack of clarity on the other elements of the offence, such as the meaning of indecency or gross offensiveness. This in turn can make it difficult to know when a defence submission that the message was sent and intended "just as a joke" will succeed or not.

Exclusions

4.106 Section 127(4) of the CA 2003 excludes from the scope of the offences in sections 127(1) and (2) "anything done in the course of providing a programme service (within the meaning of the Broadcasting Act 1990 (c. 42)").

4.107 A number of specific offences apply to those responsible for programme services,[84] which partly explains such exclusions. Those providing programme services can also face regulatory action, if the content of programmes contains certain prohibited material,[85] and financial penalties can be imposed if duties concerning harmful material are breached by programme service providers.[86]

4.108 However, the exclusions do raise a number of questions about the criminalisation rationale behind some of the proscribed behaviour in section 127, as well as the practical scope of their operation as capabilities of providing programme services develop in the modern telecommunications environment.

4.109 First, it is questionable why some of the proscribed behaviours within section 127 do not apply to communications over programme services, but do apply to communications by ordinary members of the public over the internet. For example, there is no specific

---

83 *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [38].

84 See, eg Obscene Publications Act 1959, ss 2 and 1(4), and Public Order Act 1986, ss 22 and 29F.

85 See for example the meaning of "harmful material" in the context of on-demand programme services in section 368E of the Communications Act 2003.

86 Communications Act 2003, ss 368J, 368I, 368E. The amount of the financial penalty is a maximum of 5% of the provider's applicable qualifying revenue, or £250,000, whichever is the greater amount. For the financial penalties for the Broadcasting Acts, see Communications Act 2003, Sch 13.

offence of being grossly offensive in a programme service, or sending indecent messages or other matter in this form.[87] It may be thought that regulatory enforcement will suffice where this occurs in programme services,[88] but if it is not a criminal offence to broadcast grossly offensive or indecent material to the public in a context where it may be known that there will be millions of viewers or listeners, this raises the question of why it is a criminal offence in the context of section 127.

4.110 Secondly, the definition of programme services in the Broadcasting Act 1990 could mean that there are some unintended lacunae in the scope of the section 127 offences. While the exclusion in section 127(4) is aimed at those "providing a programme service", technological developments have meant that ordinary members of the public can, with relative ease, "provide" programme services online, which would arguably come within some of these definitions of "programme services".

4.111 The definition of "programme service" is quite complex, and has a much broader remit than traditional television and radio programme services.

4.112 Section 201(1) of the Broadcasting Act 1990 (as amended) defines a programme service as any of the following services, whether it is, or requires to be, licensed:

> (aa) any service which is a programme service within the meaning of the Communications Act 2003;
>
> (c) any other service which consists in the sending, by means of an electronic communications network (within the meaning of the Communications Act 2003), of sounds or visual images or both either –
>
> > (i) for reception at two or more places in the United Kingdom (whether they are so sent for simultaneous reception or at different times in response to requests made by different users of the service);
> >
> > or
> >
> > (ii) for reception at a place in the United Kingdom for the purpose of being presented there to members of the public or to any group of persons.

4.113 The latter (section 201(1)(c)) is a remarkably broad definition. As has been outlined above in relation to the *Chambers* case, the words "sending by means of an electronic communications network" can refer – at least in the context of section 127 – to any form of communication over the internet, such as email, blogs or social media posts.

4.114 For example, a "V-logger" (video blogger) who regularly posts about a particular topic containing proscribed visual images on a video sharing website, could argue that they

---

87 Section 1(4)(a) of the Indecent Displays (Control) Act 1981 contains an exclusion for television broadcasting services and other television programme services, but the offence in section 1 of the Act would apply to other programme services.

88 See the Ofcom Broadcasting Code, s 2, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0005/100103/broadcast-code-april-2017.pdf; and Communications Act 2003, s 319(2)(a),(f), and (l).

are providing a "service", consisting of sounds and visual images, and the videos would be sent, for example, for reception at two or more places in the United Kingdom.[89]

4.115 Even in an encrypted messaging group, where one person is updating "users" regularly with a particular form of proscribed content (for example, "grossly offensive" messages), this may also come within the definition of a programme service in section 201(1)(c), due to the operation of section 202(5) of the Broadcasting Act 1990.[90]

4.116 The historical context and regulatory background of the definition of programme services would, however, suggest that these definitions of programme services are not as broad as indicated by this literal interpretation. The interpretation of a "programme service" would be determined by reference to European Union law, specifically the concept of an "audiovisual media service", as defined in article 1(1)(a) of the Audiovisual Media Services Directive.[91]

4.117 The definition of a programme service in section 201(1) of the Broadcasting Act 1990 also incorporates the definition of a programme service in the CA 2003, where it is

---

89 Note that the definition of a programme service does not apply in certain situations, outlined in in section 201(2A) and section 201(2B) of the Communications Act 2003, but these do not appear to apply to the scenario just outlined. Sections 201(2A)(a) and 201(2B)(a) of the Broadcasting Act 1990 exclude "two-way" services within the meaning of sections 248(4) and 232 of the Communications Act 2003 respectively. The latter section is relevant to the above scenario. Section 232(5) of the Communications Act 2003 defines a two-way service for the purposes of section 232 as a service that is "provided by means of an electronic communications network and an essential feature of the service is that the purposes for which it is provided involve the use of that network, or part of it, both – (a) for the transmission of visual images or sounds (or both) by the person providing the service to users of the service; and (b) for the transmission of visual images or sounds (or both) by those users for reception by the person providing the service or by other users of the service". Therefore, if one of the purposes of the service does not involve the transmission of visual images or sounds (or both) by users as an essential feature of the service, it is not a two-way service, which means it could be a programme service within s 201(c) of the Broadcasting Act 1990. In other words, if the service only facilitates users viewing the "v-logs" and does not allow users to share content, it would therefore not constitute a two-way service, and could be a programme service that is excluded from the scope of section 127 of the Communications Act 2003 by section 127(4).

90 Section 202(5) of the Broadcasting Act 1990 states "it is hereby declared that, for the purposes of determining for the purposes of any provision of this Act whether a service is – (a) capable of being received, within the United Kingdom or elsewhere, or (b) for reception at any place or places, or in any area, in the United Kingdom, the fact that the service has been encrypted to any extent shall be disregarded."

91 (2010/13/EC). The key elements of this definition are:

1. That it is a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union. Article 57 specifies that a service within the meaning of the Treaties are those that "normally provided for remuneration, in so far as they are not governed by the provisions relating to freedom of movement of goods, capital and persons."
2. That it is under the editorial responsibility of a media service provider (defined in article 1(1)(d)).
3. The principal purpose of the service is the provision of programmes to the general public by electronic communications networks in order to inform, entertain or educate.

For example, a V-logger may not, therefore, be providing a programme service unless they are providing the service for remuneration. In the online space, this could, however, quite easily occur through advertising revenues, or subscription costs paid by a V-logger's followers through sites like "Patreon" (https://www.patreon.com).

An audiovisual media service can also mean an "audiovisual commercial communication" within the meaning of Article 1(1)(h).

defined as "(a) a television programme service; (b) the public teletext service; (c) an additional television service; (d) a digital additional television service; (e) a radio programme service; or (f) a sound service provided by the BBC."[92]

4.118 Although on-demand programme services are defined separately[93] and not found in the general definition of a "programme service" in section 405(1) CA 2003, they would constitute a "programme service within the meaning of the Communications Act 2003" for the purposes of section 201 of the Broadcasting Act 1990.[94] This would also mean that anything done in the course of providing such a programme service would be outside the scope of the offences in section 127.

4.119 A recent adjudication by Ofcom illustrates how even those maintaining a Youtube channel may provide an on-demand programme service within the meaning of the CA 2003.[95]

4.120 Therefore, while the exclusion in section 127(4) does not appear to have been tested yet in the courts, there may well be cases in which individuals argue that their conduct is not an offence under section 127 as they are providing "programme services".[96] In this situation there would clearly be countervailing considerations: it could mean, for example, that they are not complying with other regulatory obligations, such as the requirement to provide advance notification to the appropriate regulatory authority,[97] and for their service not to contain harmful material.[98] This could result in enforcement action and financial penalties, which may or may not be dissuasive depending on the context and the person's situation.

4.121 This is also an important consideration for prosecutors. If a section 127 offence is charged and prosecuted, rather than an alternative offence under, for example, the Public Order Act 1986 or the Obscene Publications Act 1959, but a defence argument succeeds on section 127(4), this could mean that the individual cannot be re-prosecuted,[99] even if the latter offences were committed in fact.

---

92 Communications Act 2003, s 405(1).

93 The definition of an "on-demand programme service" has the meaning given by section 368A(1) of the Communications Act 2003.

94 See Article 1(1(g) of the Audiovisual Media Services Directive (2010/13/EC).

95 See "Resolved: Rule 1: Notification of intention to provide an On Demand Programme Service" (5 June 2017) 30 *Ofcom Broadcast and on Demand Bulletin* 43, p 43. For discussion see L Logan, *When is a Youtube Channel an on-demand programme service that needs notifying to Ofcom* (15 November 2017), available at: https://www.simkins.com/when-is-a-youtube-channel-an-on-demand-programme-service-that-needs-notifying-to-ofcom/.

96 Once evidence of this is raised, it would be for the prosecution to disprove.

97 See, eg Communications Act 2003, s 368BA, in the context of on-demand services.

98 See, eg Communications Act 2003, s 368E, in the context of on-demand services.

99 The re-prosecution would be barred on the basis of the *autrefois acquit* principle or as an abuse of process if a different offence is charged.

Time limits

4.122 The Criminal Justice and Courts Act 2015 extended the time limit for bringing proceedings under section 127 from six months to three years from the date of the offence.[100] This is a significant departure from the usual rule applicable to summary only offences.[101] Section 127(5) now states:

> An information or complaint relating to an offence under this section may be tried by a magistrates' court in England and Wales or Northern Ireland if it is laid or made –
>
> (a) before the end of the period of 3 years beginning with the day on which the offence was committed, and
>
> (b) before the end of the period of 6 months beginning with the day on which the evidence comes to the knowledge of the prosecutor which the prosecutor considers sufficient to justify proceedings.

4.123 This means that a prosecution will be time-barred unless charged within three years of the commission of the alleged offence, and within six months of the prosecutor having knowledge of sufficient evidence to justify proceedings.[102]

4.124 This extended period for bringing prosecutions under sections 127(1) and (2) has been in force since 13 April 2015,[103] and only applies in relation to an offence committed on or after this day.[104]

4.125 Where a prosecutor issues a certificate as to the date on which evidence sufficient to justify proceedings comes to their knowledge,[105] section 127(7) dictates that this is treated as conclusive evidence of that fact. This means that a prosecutor will not have to give evidence as to their knowledge, and no evidence will be heard on the issue in any criminal proceedings. Where a certificate has not been issued by a prosecutor, these timings and such matters could clearly be contested at trial.

---

100 Communications Act 2003, s 127(5), as inserted by Criminal Justice and Courts Act 2015, s 51(1).

101 Magistrates' Courts Act 1980, s 127(1). Other statutory exceptions do exist. See, eg Road Traffic Offenders Act 1988, s 6, and Animal Welfare Act 2006, s 31.

102 The latest Crown Prosecution Service guidelines on prosecuting cases involving communications sent via social media state that evidence sufficient to justify proceedings, means evidence that the "Full Code Test" is met. The Full Code Test requires that prosecutors satisfy both an evidential and public interest stage in deciding whether or not to prosecute, see Crown Prosecution Service, *The Full Code Test*, available at https://www.cps.gov.uk/publication/full-code-test.

103 The Criminal Justice and Courts Act 2015 (Commencement No. 1 Saving and Transitional Provisions) Order 2015, art 3 and sch 1.

104 The Criminal Justice and Courts Act 2015, s 51(1).

105 According to the latest Crown Prosecution Service guidelines on prosecuting cases involving communications sent via social media, evidence sufficient to satisfy the prosecutor means that the Full Code Test is met.

4.126 The latest CPS guidelines on prosecuting cases involving communications sent via social media has specific guidance for prosecutors on this extended time limit.[106]

4.127 In practice, there will be two significant issues which arise in the prosecution of offences under section 127 of the CA 2003. First, there is the question of identifying precisely "the day on which the offence was committed". Secondly, there is a question of who is the "prosecutor" with responsibility for determining whether a prosecution should be brought, and when sufficient evidence came to their attention.

4.128 On the first issue, the question arises as to whether a "sending by means of a public electronic communications network" could be a continuing act. For example, if someone writes a blog post and publishes it by uploading it to a server (whether operated by them or another), the message or matter contained within it will be "sent" over public electronic communications networks every time it is accessed by another person. This "sending" could occur years after the initial publication, and it could be argued that upon every access, the message or matter was sent (or "caused" to be sent for the purposes of section 127(1)(b) and 127(2)(b)), by the initial blog post writer. In the context of the strict liability rule in the Contempt of Court Act 1981, this is effectively the interpretation that has been adopted by the courts; where material is accessible online, "time of publication" refers to the entire period during which the material is accessible.[107]

4.129 While there is no authority on the point, it is unlikely that the courts would accept such an interpretation in the very different context of the section 127(7) time-limit.

4.130 First, the extended three-year time limit is already a significant departure from the usual six month rule for summary only offences and such an interpretation would have the practical effect of rendering nugatory any time limit at all. Individuals could be prosecuted for as long as the content is accessible. This could mean that an individual who sent messages that were not considered "indecent" at the time of initial "sending" and publishing, could find that they are committing a criminal offence a decade or more later, when understandings of indecency may have changed.[108]

4.131 Secondly, it could involve treating offenders differently depending on the medium over which their communications were sent. The day of the offence of a grossly offensive private message on a social media application may be the day it was initially sent. However, regarding messages published more generally, the day of the offence would turn on the actions of third parties (who subsequently access the content).

4.132 For sections 127(1)(a) and 127(2)(a) the more likely interpretation of the "day on which the offence was committed" is the day when the message or other matter was initially sent over a public electronic communications network. In the context of social media

---

106 When confusion arises, the Crown Prosecution Service usually produces publicly available guidelines to enhance understanding of the existing law. While these guidelines may assist with charging decisions, they do not themselves have the force of law.

107 See *HM Advocate v Beggs (No 2)* [2002] SLT 139 and *Harwood* [2012] EW Misc 27 (CC), *Attorney General v Associated Newspaper Ltd and another* [2011] EWHC 418; [2011] 1 WLR 2097 at [28]. The Law Commission has previously made recommendations on this issue in our report Contempt of Court (1): Juror Misconduct and Internet Publications (2013) Law Com No 340.

108 This would also clearly create difficulties for the principle of legality and the rule against retroactivity.

communications, this can often be quite straightforward to establish, as the postings will be marked and dated and can be verified with the social media provider. However, many difficulties may arise in demonstrating when a message was sent. For example, if a website operator or hosting provider is outside the jurisdiction and not responding to communications data requests, it may not be possible to show when a message was initially sent.

4.133 On the question of who is the prosecutor for the purposes of the time limit, there is authority in relation to time limits concerning other offences.[109] This confirms that the phrase "the prosecutor" "is not limited to prosecutors who prosecute pursuant to a power conferred by some statutory provision but applies to anyone who initiates a prosecution [for the relevant offence]".[110] More recently, the High Court confirmed – again in the context of section 31 of the Animal Welfare Act 2006 – that the prosecutor "is the individual with responsibility for deciding whether a prosecution should go forward ...".[111]

4.134 In relation to section 127 offences, police can submit reports seeking charging decisions, and can take a decision to charge without reference to the CPS. The latest CPS guidelines therefore draw on the above case-law and suggest that the police should ordinarily be treated as the relevant decision-maker (and thus the "prosecutor" for the purposes of section 127(5)) where they have taken such steps.

Territorial Jurisdiction

4.135 Neither the CA 2003 nor the MCA 1988 contain specific statutory provisions concerning jurisdiction over the offences in section 127 of the CA 2003 and section 1 of the MCA 1988.

4.136 However, the territorial ambit of the offences in the MCA 1988 had been analysed by the Law Commission and debated in Parliament. In our Poison Pen Letters report, we considered whether it could be a domestic offence to send a poison pen letter from abroad, in circumstances where it was received by, and targeted at, someone in England and Wales. We took the view that no offence would be committed in England and Wales in these circumstances,[112] reiterating the traditional territorial limitations of the criminal law at the time. While we noted the possibility to statutorily extend the ambit of the offence by providing extraterritorial jurisdiction, we had concerns about the offence becoming "unacceptably wide" and it being highly unusual for a summary only offence (as was being recommended then) to apply to conduct abroad.[113]

4.137 As noted in Chapter 2, however, the courts have recently taken a more expansive approach to territorial jurisdiction through the adoption of the substantial measure test.

---

109 See, eg Animal Welfare Act 2006, s 31.

110 *Lamont-Perkins v RSPCA* [2012] EWHC 1002 (Admin); (2012) 176 JP 369 at [26].

111 *R v Woodward and others* [2017] EWHC 1008 (Admin); [2017] *Criminal Law Review* 884.

112 Poison Pen Letters (1985) Law Com No 147, para 4.43.

113 Poison Pen Letters (1985) Law Com No 147, para 4.44. In Parliamentary debates concerning the Malicious Communications Act 1988, extraterritorial jurisdiction was again considered. Then Minister of State for the Home Office, John Patten MP, accepted a domestic offence would not be committed if the communication was sent from abroad, even where received in England or Wales, and noted that while extradition could be considered for alternative offences, it may not be available unless those offences were extradition crimes: see *Hansard* (HC), 12 February 1988, vol 127, col 624.

This means that where section 127 of the CA 2003 or section 1 of the MCA 1988 offences have a foreign dimension, they could nevertheless constitute an offence in England and Wales if a substantial measure of the activities constituting the crime take place here.

4.138 Uncertainty exists in relation to this approach, as it applies to internet activities. In the context of section 127 of the CA 2003, for example, a communication could be routed through public electronic communication networks in England and Wales, but involve two individuals that are outside the jurisdiction and have no connections with England or Wales whatsoever. To hold that such a communication was a domestic offence on the basis of the substantial measure test could be difficult to sustain as a matter of substantive law. It would also be an expansive approach that would generate the problems of jurisdictional concurrency.

4.139 On the other hand, if an individual sent a proscribed communication while physically in England or Wales, or targeted a communication at someone in England and Wales from abroad and it was received by them here, it will be more likely that a court would take the view that a substantial measure of the activities constituting the crime took place here. Moreover, from an enforcement perspective, it is only where a significant domestic nexus like this exists that law enforcement will be likely to pursue a prosecution.

CPS Prosecution Guidance

4.140 The CPS has recently updated its guidance to prosecutors in relation to "prosecuting cases involving communications sent via social media".[114]

4.141 It states that in considering the use of the communications offences under section 1 of the MCA 1988 or section 127 of the CA 2003, prosecutors should first consider whether another "substantive offence" has also been committed – for example, stalking, harassment, threat to kill etc, and pursue these offences rather than communications offences.

4.142 If communications offences are to be prosecuted, CPS guidance states that section 127 of the CA 2003 offences are preferable for communications made over a public electronic communications network (provided that the maximum penalty of six months is adequate in the circumstances). However, section 1 of the MCA 1988 will be the only available offence where a public electronic communication has not been used to make the communication. The guidance also notes that the fault element in section 1 of the MCA 1988 is more stringent, and as we note above at paragraph 4.25, there is an argument that certain forms of communication that are not directed at "another person" may fall outside the scope of the offence under section 1 of the MCA 1988.

4.143 In considering whether prosecutors should exercise the discretion to prosecute a communications offence, further guidance is provided.

---

114 Crown Prosecution Service, *Social Media - Guidelines on prosecuting cases involving communications sent via social media* (21 August 2018), available at https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media.

4.144 First, in weighing whether prosecution is proportionate and justified in light of the right to freedom of expression under Article 10 of the European Convention on Human Rights (ECHR), CPS guidance states that the relevant communication should be 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 or "give and take".

4.145 Then in considering whether a prosecution is in the public interest, CPS guidance lists the following as relevant factors for consideration:

- the likelihood of re-offending;
- the suspect's age or maturity;
- the circumstances of and the harm caused to the victim, including whether they were serving the public, whether this was part of a coordinated attack ("virtual mobbing"), whether they were targeted because they reported a separate criminal offence, whether they were contacted by a person convicted of a crime against them, their friends or family;
- whether the suspect has expressed genuine remorse;
- whether swift and effective action has been taken by the suspect and/or others for example, service providers, to remove the communication in question or otherwise block access to it;
- whether the communication was or was not intended for a wide audience, or whether that was an obvious consequence of sending the communication; particularly where the intended audience did not include the victim or target of the communication in question;
- whether the offence constitutes a hate crime.

4.146 The effect of this guidance is that even where reported to law enforcement, not all conduct that might technically meet the broad terms of section 1 of the MCA 1988 or section 127 of the CA 2003 offences is actually prosecuted. For example, it may be judged that to do so would unreasonably infringe on freedom of expression; distasteful humour is a typical example. Alternatively, the circumstances of the offender may lead prosecutors to consider that the public interest would not be served by pursuing a criminal penalty; for example, where the offender is young and remorseful and their conduct did not cause substantial harm.

4.147 However, in subsequent Chapters – in particular Chapter 5 on grossly offensive communications – we suggest that the guidelines may not be enough to resolve the interpretative challenges that are arising in the online context. As discussed further in Chapter 5, CPS guidelines do not of themselves have the force of law, but rather provide assistance with charging decisions. Where the underlying proscribed behaviour is broad, malleable, and ill-defined, CPS guidelines may simply not suffice, leaving too much to the charging discretion of prosecutors.

CONCLUSION

4.148 The above outline of section 1 of the MCA 1988 and section 127 of the CA 2003 has shown considerable overlap between these two offences in the online context and the purpose of this has not been convincingly demonstrated or explained.

4.149 In *Collins* Lord Bingham explained that the aim of the offence under section 1 of the MCA 1988 is to "protect people against receipt of unsolicited messages which they may find seriously objectionable".[115]

4.150 On the other hand, "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".[116] Lord Brown agreed that "section 127(1)(a) is indeed intended to protect the integrity of the public communications system".[117]

4.151 These observations about the purpose of section 127 of the CA 2003 appear ill-suited in certain respects. Most public electronic communications networks today are not actually provided and funded by the public for the benefit of the public; they are rather created and operated by corporations, who generate revenue from their use. As Walden observes, Lord Bingham's explanation "does not appropriately describe our modern liberalized, competitive and largely non-publicly funded communications industry and therefore seems an unsatisfactory basis upon which to distinguish the two statutes and to interpret [section 127]".[118] Moreover, prohibiting grossly offensive or indecent communications cannot protect the "integrity" of the public communications system as Lord Brown stated, at least in terms of protecting the security of communications and the technical operation of the system(s). Even as a description of ensuring the moral integrity of communications over public communications networks, enforcement of section 127 is now more orientated towards ensuring the propriety of communications on platforms operating through public communications networks (like Twitter), rather than anything directly to do with the networks, or their operators.

4.152 As outlined above, one of the justifications for having separate offences in section 1 of the MCA 1988 and the telecommunication offences which became section 127 of the CA 2003, was because it was intended that section 1 of the MCA 1988 would not apply to electronic communications. When section 1 of the MCA 1988 was amended in 2001 to extend to electronic communications, it appears there was insufficient attention given

---

115 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [7].

116 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [7].

117 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [7].

118 Ian Walden, *Computer Crime and Digital Investigations* (2nd ed, 2016), para 3.203.

to the adequacy of other offences (such as section 43 of the Telecommunications Act 1984) or the Law Commission's reasoning for having two sets of offences. The overlap that now exists across these offences is confusing, as illustrated in the case referred to in paragraph 4.26, and largely unexplained.

4.153 This suggests there would be considerable benefit in reviewing whether the offences in section 127 of the CA 2003 and section 1 of the MCA 1988 should be amalgamated into one coherent set of offences.

4.154 This Report will also show that elements of these offences are broadly defined and rather ambiguous on some of the proscribed speech, with much left to the courts and prosecutorial discretion.

4.155 While the breadth and flexibility afforded by the communications offences certainly has advantages, as we explore further in later Chapters, it also creates ambiguities and uncertainties, such as the meaning of indecency, obscenity and gross offensiveness, which are undesirable in the context of criminal law.

4.156 The time is also apt for a reconsideration of the thresholds required for abusive and offensive communications to constitute criminal offences. In the appendices to this Report we have outlined alternative approaches adopted in other jurisdictions, such as communication offences which focus on the harm caused to victims. In the final Chapter of this Scoping Report, we recommend that a public consultation on a proposed redesign of these offences should form a part of Phase 2 of this work.

Chapter 5: Gross offensiveness

INTRODUCTION

5.1 As Chapter 4 explained, section 127(1)(a) of the Communications Act 2003 ("CA 2003") makes it an offence to send by means of a public electronic communications network, a message or matter that is "grossly offensive". It is also an offence to cause such material to be sent (under section 127(1)(b) of the CA 2003).

5.2 The Malicious Communications Act 1988 ("MCA 1988") also criminalises sending another person a letter, electronic communication or article of any description which conveys a message that is grossly offensive (section 1(1)(a)(i)), or sending another person any article or electronic communication which is, in whole or part, of a "grossly offensive" nature (section 1(1)(b)).

5.3 The elements of these offences were discussed in greater detail in Chapter 4. The purpose of this Chapter is to analyse the meaning of the term "grossly offensive" in the context of section 127 of the CA 2003 and section 1 of the MCA 1988.

5.4 Of all the proscribed behaviours caught by section 127 of the CA 2003 and section 1 of the MCA 1988, this variant of the offences is arguably the most contentious and contested. There are no explicit definitions of "grossly offensive" in section 127(1) of the CA 2003 or section 1 of the MCA 1988; this is left to judicial interpretation.

5.5 Its enforcement is often criticised by academics,[1] journalists,[2] lawyers,[3] and human rights organisations such as Big Brother Watch[4] and Open Rights Group.[5] This is particularly striking given that statutory offences relating to "grossly offensive" communications have existed for over a hundred years. In the 1980s, when we consulted on poison pen letters, "no criticisms were made in relation to the term 'grossly offensive'" and we therefore recommended its incorporation into the offence that became section 1 of the MCA 1988.[6]

---

1 See eg, L Edwards, *Section 127 of the Communications Act 2003: Threat or Menace?* (October 2012), available at http://blogs.lse.ac.uk/mediapolicyproject/2012/10/19/section-127-of-the-communications-act-2003-threat-or-menace/.

2 See eg, D A Green, *The menace of section 127: the wider implications of the Twitter Joke Trial* (17 November 2010), available at https://www.newstatesman.com/blogs/the-staggers/2010/11/section-127-paul.

3 See eg, G Smith, *From telegram to tweet – Section 127 and all that* (4 March 2015), available at https://inforrm.org/2015/03/04/from-telegram-to-tweet-section-127-and-all-that-graham-smith/.

4 See eg, Big Brother Watch, *Careless Whispers: How speech is policed by outdated communications legislation: A Big Brother Watch Report* (February 2015), available at https://bigbrotherwatch.org.uk/2015/02/careless-whisper-how-speech-is-policed-by-outdated-communications-legislation/.

5 See eg, Open Rights Group, *Submission to DPP Consultation on Social Media Prosecutions* (2012), available at https://www.openrightsgroup.org/about/reports/submission-to-dpp-consultation-on-social-media-prosecutions.

6 Poison Pen Letters (1985) Law Com No 147, para 4.15.

5.6 The landscape has clearly changed since then, and the major technological revolution behind this has been the development of the internet and social networking. As Chapter 1 described, the scale of one-to-many communications increased with this technological development, and so did the ability to cause offence to others. Many now question whether the offences in section 1 of the MCA 1988 and section 127 of the CA 2003 (which we examine in more detail in Chapter 4) are equipped to deal with this new and more complex environment, pointing to how the predecessor offences to section 127 of the CA 2003, in particular, were more orientated towards addressing grossly offensive one-to-one communications.

5.7 Below, we illustrate why prosecutions relating to grossly offensive communications have become so challenging. We begin by considering some of the justifications for criminalising "grossly offensive" speech. We then trace the historical development of the offences relating to grossly offensive communications.

5.8 The next section of this Chapter considers some of the key cases that have analysed the meaning of "grossly offensive" communications in the context of section 1 of the MCA 1988, and section 127 of the CA 2003. This reveals that there is little in terms of judicial guidance as to when speech or communication will cross the line from being merely "offensive" to being "grossly offensive".

5.9 We next consider how the Crown Prosecution Service ("CPS") social media guidelines have impacted on the prosecution of communications offences relating to grossly offensive speech, and find that a number of difficulties continue to exist in this area.

5.10 In the final section, we briefly consider case law where offences relating to "grossly offensive" communication have been challenged on freedom of expression grounds.

WHY SHOULD "GROSSLY OFFENSIVE" COMMUNICATION BE CRIMINAL?

5.11 The criminalisation of "grossly offensive" conduct has been justified primarily by the "Offence Principle".[7]

5.12 Feinberg referred to offence as an affront to people's sensibilities; distinct from the "harm principle".[8] "Offensiveness" for Feinberg involved emotions such as:

> Passing annoyance, disappointment, disgust, embarrassment, and various other disliked conditions such as fear, anxiety, and minor ("harmless") aches and pains ...[9]

5.13 There is a distinction between what is merely "offensive" and offensive conduct that could be criminal. As Feinberg notes, conduct can be merely "offensive" without any

---

7 The two main criminalisation principles are harm and offence. But these are contested; see, eg A Ellis, "Offense and the Liberal Conception of the Law" (1984) 13(1) *Philosophy and Public Affairs* 3; E Haavi Morreim, "The Concept of Harm Reconceived: A Different Look at Wrongful Life" (1988) 7(3) *Law and Philosophy* 33; and J Kleinig, "Crime and the Concepts of Harm" (1978) 15(1) *American Philosophical Quarterly* 27.

8 Note there are numerous criticisms of the offence principle, that it is in fact a subset of the harm principle. See also T Petersen, "No Offense! On the Offense Principle and Some New Challenges" (2016) 10 *Criminal Law and Philosophy* 355; and DW Shoemaker "Dirty words and the offense principle" (1999) 19(5) *Law and Philosophy* 545.

9 J Feinberg, *The Moral Limits of the Criminal Law, Volume 2 - Offense to Others* (1988) p 1.

wrongdoing on the part of the person engaging in the conduct. One can, for example, be disgusted by the blood pouring from an innocent person's wound. However, the person who is wounded is not engaging in any sort of wrongdoing in causing the person to witness that and feel offended, and it would not make sense for this to be a criminal offence. This differs from what Feinberg terms "wrongfully offending" others; when offence is caused by the wrongful conduct of others.

5.14 The theory, therefore, suggests that before offensive behaviour can be criminalised it must be both an affront to sensibility *and* "something else" which aggravates the conduct such that it justifies becoming a criminal offence.[10] What should suffice or be necessary for this "something else" has, however, differed amongst theorists.

5.15 Feinberg, for example, considers four factors that justify state intervention into offensive conduct. First, the magnitude of the conduct (including its intensity, duration and extent); secondly, that the offence becomes more serious the harder it is for those who are offended to avoid it; thirdly, whether the offence was voluntarily incurred; and finally, that the seriousness of offence should be discounted if a person has an "abnormal susceptibility to offense".[11]

5.16 Shoemaker suggests that this list is incomplete, adding that there should be a "reasonableness condition", to avoid criminalising conduct where, although offence may be taken to it, such offence is unreasonable.[12]

5.17 Von Hirsch says that the "something else" should involve a list "of valid normative reasons for objecting to the conduct". He considers that these "reasons" might involve, for example, where the offensive conduct intrudes on others' privacy;[13] when the conduct is insulting, or demeans the character of another such that it is "grossly derogatory";[14] or where it interferes with "others' ability to use and enjoy common resources and facilities".[15] Wrongdoing may also consist of "treating other persons with a gross lack of respect or consideration".[16] Von Hirsch suggests that "such reasons should be made explicit, and … be subjected to crucial scrutiny, before conduct may be deemed offensive. It is not enough that the conduct be widely disapproved of, or that it

---

10 A von Hirsch, "The Offence Principle in Criminal Law: Affront to Sensibility or Wrongdoing?" (2000) 11(1) *King's Law Journal* 78, p 83.

11 J Feinberg, *The Moral Limits of the Criminal Law, Volume 2 - Offense to Others* (1988), p 35.

12 DW Shoemaker, "Dirty words and the offense principle" (1999) 19(5) *Law and Philosophy* 545, p 553; a similar standard was proposed in D Vandeveer, "Coercive Restraint of Offensive Actions" (1979) 8(2) *Philosophy and Public Affairs* 175, p 181. However, Feinberg did not see it necessary to include such a condition: see J Feinberg, *The Moral Limits of the Criminal Law, Volume 2 - Offense to Others* (1988), p 35.

13 A von Hirsch, "The Offence Principle in Criminal Law: Affront to Sensibility or Wrongdoing?" (2000) 11(1) *King's Law Journal* 78, p 83.

14 A von Hirsch, "The Offence Principle in Criminal Law: Affront to Sensibility or Wrongdoing?" (2000) 11(1) *King's Law Journal* 78, p 84.

15 A von Hirsch, "The Offence Principle in Criminal Law: Affront to Sensibility or Wrongdoing?" (2000) 11(1) *King's Law Journal* 78, p 85.

16 A von Hirsch and AP Simester, "Regulating Offensive Conduct through Two-Step Prohibitions" in A von Hirsch and AP Simester (eds) *Incivilities: Regulating Offensive Behaviour* (2006) p 119.

infringes certain traditional taboos".[17] This suggests the need to impose explicit and agreed limitations on the prohibition of offensive conduct.

5.18 The lack of such explicit limitations distinguishes principles governing criminalising causing offence from causing harm, which has "self-limitations" before conduct gives rise to criminal liability. For example, while harm can be caused in many ways and in varying degrees, instigating harm only becomes a crime when certain interests of a person are infringed upon or taken away (for example, "by transgressing on my physical person, taking or damaging my property, injuring my good name").[18] As von Hirsch warns, "unless care is taken, this self-limitation is lost when formulating the offense principle". Without similar limitations, some commentators believe we risk over criminalising offensive conduct.

5.19 In England and Wales, the statutory limitation imposed on offensive conduct in the context of communications offences is the word "grossly", which suggests an aggravating element that distinguishes such communications from mere offensiveness. However, exactly what that aggravating element may be and when that threshold from offence to gross offence may be crossed is currently a matter of judicial interpretation.

HISTORICAL DEVELOPMENT OF "GROSSLY OFFENSIVE" COMMUNICATIONS OFFENCES

"Gross offensiveness" in the Post Office Protection Act 1884

5.20 The concept of "gross offensiveness" in the criminal law in England and Wales has its origins as far back as the 1800s. Section 4(c) of the Post Office Protection Act 1884, for example, provided for an offence of sending or attempting to send a postal packet which "has on such packet, or on the cover thereof, any words, marks, or designs of an indecent, obscene, or grossly offensive character". The concept was initially designed to protect public morality, rather than protecting a particular person from offence.[19]

5.21 However, the inclusion of the words "grossly offensive" were firmly challenged in the course of passing this Act. For example, Charles Warton MP argued the term was too vague and open to misinterpretation, and that the penalty was too severe for the offence. Mr Warton:

> was afraid that the words "grossly offensive" might be taken to mean something very different to indecent or obscene… it might happen that one man would use words—for instance, he might write "swindler" or "liar" upon the outside of a letter—which were not really indecent or obscene, only what they would call vulgar … the words "grossly offensive" might be taken to mean something that was extremely offensive to the

---

17 A von Hirsch, "The Offence Principle in Criminal Law: Affront to Sensibility or Wrongdoing?" (2000) 11(1) *King's Law Journal* 78, p 85.

18 A von Hirsch, "The Offence Principle in Criminal Law: Affront to Sensibility or Wrongdoing?" (2000) 11(1) *King's Law Journal* 78, p 86.

19 *Hansard* (HC), 9 August 1884, vol 292, col 372.

person who received it, although it did nothing more than lacerate the feelings of the person receiving it.[20]

5.22 His concerns were somewhat realised; in 1913, John Cole was convicted under the 1884 Act for sending postcards to local officials calling an alderman an "insurance swindler" which was found to be grossly offensive.[21] From the outset, there has been confusion and criticism over where the threshold is crossed and when, or why, matter is considered grossly offensive, rather than simply vulgar abuse.

"Gross offensiveness" since the 1884 Act

5.23 The term has since been adopted consistently through numerous communication offences in England and Wales (with one exception, noted further below). For example, in relation to postal packets, the Post Office Amendment Act 1908; for telephony and telegrams, section 10(2)(a) of the Post Office (Amendment) Act 1935 and section 66(a) of the Post Office Act 1953; with regard to public telecommunications, section 78 of the Post Office Act 1969, section 49(1)(a) of the British Telecommunications Act 1981 and section 43(1)(a) of the Telecommunications Act 1984. The only significant difference between these Acts was the evolving means of communication.[22]

5.24 The exception to this legislative development were the offences in sections 85(3) and (4) of the Postal Services Act 2000, which removed the term "gross offensiveness". The offences related only to indecent or obscene material; it is not clear why the term "gross offensiveness" was removed from the formula used in its predecessor offences.

5.25 A House of Commons debate in 1987 considered whether the test for obscenity in the Obscene Publications Bill (never enacted) should be extended to include a new test based on gross offensiveness. This test, it was said, would apply to articles "which a reasonable person would regard as grossly offensive by reason of the way in which they portray violence, horror, sex or drugs ... the new test would also apply to sex aids, bondage items and so on".[23] This suggests that the portrayal of violence, horror, sex or drugs were factors – at least at that time – that might help to determine whether a message was "grossly offensive".

5.26 In attempting to define the term, and reflecting the literature on the offence principle, Gerald Howarth MP stated in the 1987 House of Commons debate that "the grossly offensive requirement requires grave affront to have been caused, and a jury would have to be persuaded of that. It is not sufficient for one person, who deems himself to be reasonable, and who says that he has been grossly offended, to persuade a jury".[24]

---

20 *Hansard* (HC), 09 August 1884, vol 292, col 371.

21 See G Smith, *From telegram to tweet – Section 127 and all that* (4 March 2015), available at https://inforrm.org/2015/03/04/from-telegram-to-tweet-section-127-and-all-that-graham-smith/.

22 Discussed in *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [6].

23 *Hansard* (HC), 3 April 1987, vol 113 col 1327.

24 *Hansard* (HC), 3 April 1987, vol 113 col 1328.

He also said that "the concept has the vital merit of being able to respond to changes in public perception of what is acceptable or unacceptable".[25]

5.27 However, there was still confusion as to its meaning. Gerald Howarth MP had qualms with the term "gross" in relation to "gross offensiveness", noting that "it is a qualitative term about which I am not clear".[26] Norman Buchan MP also criticised the term for having a "vague definition" which, in relation to broadcasting, would "inhibit the freedom of the broadcaster".[27] Clare Short MP also found the grossly offensive test "very worrying";[28] and Ian Mikardo MP criticised it for being "vague, indeterminate and subjective".[29] There was confusion over whether "gross" meant "extreme" as opposed to "obvious".

5.28 Although gross offensiveness was removed as an element of the offence relating to postal packets in the context of section 85(3) and (4) of the Postal Services Act 2000, it was retained for the purposes of section 1 of the MCA 1988 and section 127 of the CA 2003.

The Malicious Communications Act 1988

5.29 As explained in Chapter 4, in 1985 the Law Commission produced a report recommending the introduction of the Malicious Communications Act in response to "poison pen letters", including the criminalisation of communications that were "grossly offensive".

5.30 We recommended the offence should apply only where there was a specific intent element (drafted in the legislation as intent to cause distress or anxiety); and even then, not in relation to purely spoken communication.

5.31 The meaning of "gross offensiveness" in the MCA 1988 has been debated since its enactment. In the House of Lords in 1994, for example, Lord Irvine of Lairg moved that a clause should be included in section 1 of the MCA 1988, stating that "in this section the words 'grossly offensive' shall include material that is offensive on the grounds of the colour, race, nationality (including citizenship) or ethnic or national origin of the recipient or of any other person to whom the sender intends that it or its contents or nature shall be communicated".[30] This sparked debate over the meaning of "gross offensiveness" and whether, as it stood, the term included conduct that was racially offensive. Earl Ferrers DL was of the opinion that the term "can encompass a wide range of material, including that which may cause gross offence on the grounds that it attacks or vilifies the recipient's race, family, colour or origin".[31]

---

25 *Hansard* (HC), 3 April 1987, vol 113, col 1328.

26 *Hansard* (HC), 3 April 1987, vol 113, col 1339.

27 *Hansard* (HC), 3 April 1987, vol 113, col 1339.

28 *Hansard* (HC), 3 April 1987, vol 113, col 1341.

29 *Hansard* (HC), 3 April 1987, vol 113, col 1348.

30 *Hansard* (HL), 16 June 1994, vol 555, col 1917.

31 *Hansard* (HL), 16 June 1994, vol 555, col 1920.

5.32 Parliament considered again in 1994 whether a test of "gross offensiveness" should be inserted in the Obscene Publications Act 1959 ("OPA 1959"). The Rt Hon the Earl Ferrers DL argued that:

> A gross offensiveness test is at least flexible, but it seems wrong in principle to ban something just because some people, or even most people, may be offended by it. Many things may be offensive to many people, but this is not, in itself, a reason to ban them.[32]

5.33 This quotation reflects the sentiments of the literature reviewed above; that an offensive act requires additional factors before it can become a criminal offence. However, if the gross offensiveness test was considered too vague and inappropriate for the OPA 1959, it begs the question why it has been assumed appropriate for the purposes of section 1 of the MCA 1988 and section 127 of the CA 2003.

"Gross offensiveness" and the advancement of technology

5.34 Technology in the online space has now transformed the landscape to which this concept applies. The accessibility of many online communication platforms means that one-to-many communications are now common. Conversations or posts on social media, for example, may be seen by many different groups of all ethnicities, religions, social classes, ages, genders, sexualities, abilities, and more. Intended "private" online messages can also reach a much wider audience than any offline communication.[33] Research has shown that people now spend significant amounts of time online.[34]

5.35 Chapter 4 discussed the broad application of communication offences, particularly section 127 of the CA 2003. The range of communication, to which section 1 of the MCA 1988 and section 127 of the CA 2003 may apply, is vast.

5.36 Potentially "grossly offensive" communication can apply to messages which have been carefully planned and scripted, as well as spontaneous messages. It may include messages that are initially intended to be humorous, messages re-posted out of context, and communications meant for a small circle of friends but which go "viral" and become more public than intended.

5.37 Those who use the internet to communicate need clear and certain law. In this Chapter, we ask whether the concept of gross offensiveness is fit for purpose in this regard.

5.38 The next section will consider whether case law has been able to help clarify what is meant by "gross offensiveness", in the absence of a legislative definition.

---

32 *Hansard* (HL), 11 July 1994, vol 556, col 1537.

33 A Murray, *Information Technology Law: The Law and Society* (2nd ed, 2013) p 138.

34 T Tamblyn, *People in the UK Now Spend A Day Online Every Single Week* (26 April 2018), available at https://www.huffingtonpost.co.uk/entry/people-in-the-uk-now-spend-a-day-online-every-single-week_uk_5ae1b947e4b055fd7fc8ca71.

KEY CASES DEFINING "GROSS OFFENSIVENESS"

5.39 Lord Justice Sedley famously stated that "freedom only to speak inoffensively is not worth having".[35]

5.40 The most notable cases that have sought to define when material would be considered "grossly offensive" for the purposes of section 1 of the MCA 1988 and section 127 of the CA 2003, although not specifically in relation to online communication, are *DPP v Collins*[36] and *Connolly v DPP.*[37]

5.41 In *DPP v Collins*,[38] the appellant had sent numerous telephone calls and messages to Members of Parliament. Driven by his very strong views about immigration and asylum policies, he made a number of racist comments, including references to "Wogs", "Pakis" and "Black Bastards".

5.42 The magistrates dismissed the charges. In a case stated for the High Court, the magistrates gave their reasons. They stated that while Collins' communications were offensive, they could not be considered grossly offensive, and fell outside section 127 of the CA 2003.[39]

5.43 In the Queen's Bench Divisional Court, Sedley LJ and Mitting J upheld the magistrates' decision. Sedley LJ noted that the term "grossly" indicated some "added value" to mere offensiveness. This, he said, should be a question of fact based on "the standards of an open and just multi-racial society".[40]

5.44 The Judicial Committee of the House of Lords overturned the decision on appeal, concluding that the messages were "grossly offensive" because they involved language "beyond the pale of what is tolerable in our society",[41] given that public communications networks were funded by the people for the benefit of the public and that the purpose of section 127 of the CA 2003 was to prohibit communication which affronted the standards of society.

5.45 Although the House of Lords agreed there was a distinction between what is merely offensive and "grossly offensive", they did not explicitly state what that difference is. As Gillespie noted:

---

35 *Redmond-Bate v DPP* [1999] EWHC Admin 733; [1999] *Criminal Law Review* 998 at [20].

36 [2006] UKHL 40; [2006] 1 WLR 2223.

37 [2007] EWHC 237 (Admin); [2008] 1 WLR 276.

38 [2006] UKHL 40; [2006] 1 WLR 2223.

39 Note that although his communications occurred during the period between 2002 and 2004, partly prior to the enactment of section 127(1) of the Communications Act 2003, he was still charged under that provision as it was treated as if it had been effective throughout the whole period.

40 *DPP v Collins* [2005] EWHC 1308 (Admin) at [11].

41 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [11].

> This is perhaps because they believe that a tribunal of fact can readily understand the difference, but Parliament explicitly referred to "grossly offensive" and it would perhaps have been appropriate to explain the difference.[42]

5.46 The House of Lords instead agreed that this is a question of fact decided by reference to a reasonable person test.[43] The House also said that messages should take into account context and circumstances,[44] particularly as "usages and sensitivities may change over time".[45] Lord Bingham stated:

> There can be no yardstick of gross offensiveness otherwise than by the application of reasonably enlightened, but not perfectionist, contemporary standards to the particular message sent in its particular context. The test is whether a message is couched in terms liable to cause gross offence to those to whom it relates.[46]

5.47 Academics such as Gillespie and Kohl have criticised the last sentence of this quotation as suggesting that gross offensiveness may be determined by the recipient, which is at odds with the reasonable person test. This confusion was further fuelled by Lord Carswell, who considered evidence conceded by the respondent's counsel in the Divisional Court that a member of the relevant ethnic minority who heard the messages found them to be grossly offensive. He went on to conclude that:

> If one accepts the correctness of that concession, as I believe one should, then one cannot easily escape the conclusion that the messages would be regarded as grossly offensive by reasonable persons in general, judged by the standards of an open and just multiracial society.[47]

5.48 Gillespie and Kohl have argued that this inaccurately assumes that the reaction of one minority group in society is synonymous with the reasonable person.[48] While it is debatable whether Lord Carswell was doing more than simply drawing conclusions about the evidence in this particular case, it is another indication of the difficulty in defining and applying the notion of "gross offensiveness".

5.49 *DPP v Collins* demonstrates the malleability of this concept: while the Justices and High Court judges found the actions of Collins were not unlawful, the House of Lords unanimously took the opposite view and found that reasonable members of society would find the messages grossly offensive. Similar differences in interpretation have also been an issue in other cases, discussed further in the next section of this Chapter.

---

42 A Gillespie, "Case Comment: Offensive communications and the law" (2006) 17(8) *Entertainment Law Review* 236, p 237.

43 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [9].

44 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [9].

45 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [9].

46 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [9].

47 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [22].

48 See A Gillespie "Case Comment: Offensive communications and the law" (2006) 17(8) *Entertainment Law Review* 236; and U Kohl "Islamophobia, 'gross offensiveness' and the internet" (2018) 27(1) *Information and Communications Technology Law* 116.

5.50 Another key case on the interpretation of "gross offensiveness" was *Connolly v DPP.*[49] In this case, the appellant was a devout Christian who had sent photographs of aborted foetuses to three pharmacies that sold the morning-after pill. She was convicted under section 1 of the MCA 1988 for sending indecent and grossly offensive articles with the purpose of causing distress and anxiety.

5.51 On appeal by way of case stated, the appellant argued that the photographs did not cross the threshold of gross offensiveness. The High Court rejected this argument, noting that the terms "grossly offensive" were "ordinary English words"[50] and, in light of this, concluded that the lower court was entitled to find that the photographs were grossly offensive:

> We have seen the photographs. They are close-up colour photographs of dead 21-week-old foetuses. The faces and limbs are clearly visible. One of them is a close-up showing an abortion taking place. They are shocking and disturbing… In my view, it is impossible to say that no reasonable tribunal could have concluded that these images were grossly offensive within the meaning of section 1 of the 1988 Act.[51]

5.52 While the photographs were determined to be grossly offensive in these circumstances, Dyson LJ offered little in terms of further guidance as to when this threshold is reached.

5.53 The difference between "offensive" and "grossly offensive" was also discussed in the case of *Karsten v Wood Green Crown Court*.[52] In this case, a series of antisemitic calls were made to the complainant by a friend of the appellant. The appellant, although not the person who called, was heard in the background saying to the caller "ask him if he's Jewish. Ask him if he's eating kosher".[53] This message was found by the Crown Court to be offensive, but not "grossly offensive" as required by section 127 of the CA 2003. The High Court agreed:

> The Crown Court found that the words were not grossly offensive; they were certainly offensive: a nasty, malicious antisemitic comment of which the appellant should be thoroughly ashamed, but they were not menacing. The courts need to be very careful not to criminalise speech which, however contemptible, is no more than offensive. It is not the task of the criminal law to censor offensive utterances.[54]

5.54 These cases sought to develop a consistent approach to determine when a message or matter is "grossly offensive". The next section considers how the difficulties of discerning gross offensiveness also apply to the online world, and considers the extent to which the new CPS charging guidelines, relating specifically to social media, assist with these difficulties.

---

49 [2007] EWHC 237 (Admin); [2008] 1 WLR 276.

50 *Connolly v DPP* [2007] EWHC 237 (Admin); [2008] 1 WLR 276 at [10].

51 *Connolly v DPP* [2007] EWHC 237 (Admin); [2008] 1 WLR 276 at [11].

52 *Karsten v Wood Green Crown* Court [2014] EWHC 2900 (Admin).

53 *Karsten v Wood Green Crown Court* [2014] EWHC 2900 (Admin) at [1].

54 *Karsten v Wood Green Crown Court* [2014] EWHC 2900 (Admin) at [21].

ONLINE CONSIDERATIONS

5.55 The broad offence of sending a "grossly offensive" message now has the potential to capture a wide range of communication online. Social media and other online platforms have increased the opportunities for individuals to make their views and ideas accessible to a wide audience. Research has also shown that people are less inhibited online than they are offline.[55] As a result, the online user is exposed to an ever-increasing amount of material.

5.56 However, with such a vast amount of material being sent online, users of the web, particularly social media, may be confused as to what amounts to "grossly offensive" communication in law.

5.57 When confusion arises, the CPS usually produces publicly available guidelines to enhance understanding of the existing law. While these guidelines may assist with charging decisions, they do not themselves have the force of law.

5.58 To help reduce confusion around the online application of communications offences, the CPS introduced *Guidelines on Prosecuting Cases Involving Communications Sent via Social Media* in 2013. These were updated in 2016, and the latest guidelines were released in August 2018 (discussed in Chapter 4).

5.59 The next section will use real case examples to show the concerns that led to the introduction of the CPS guidelines in relation to communication on social media. It then considers whether those guidelines are now sufficient to address the challenges of applying grossly offensive provisions to cases of online communication.

5.60 The remainder of this Chapter will demonstrate the continuing difficulty in determining whether online communications are grossly offensive, despite the introduction of the CPS guidelines. Controversial prosecutions continue to arise in these cases because the underlying proscribed conduct is very broadly interpreted and the concepts are malleable. The CPS guidelines are not sufficient to avoid this, given they too are reliant on the provisions in law, and without further clarification in law, these difficulties in applying gross offensiveness will continue.

The introduction of the CPS Social Media Guidelines

5.61 Although the key cases described above sought to establish a consistent test of gross offensiveness, subsequent high-profile cases suggested that the threshold is very difficult to delineate.

---

55 See paragraphs 2.157 to 2.160. Empirical research has indicated that people are less inhibited online than they are in offline (particularly with face-to-face) communication: see, eg AN Joinson, "Disinhibition and the Internet" in Gakenbach (ed) *Psychology and the Internet: Intrapersonal, Interpersonal, and Transpersonal Implications* (2007) p 70; see also GS Mesch and G Baker, "Are norms of disclosure of online and offline personal information associated with the disclosure of personal information online?" (2010) 36(4) *Human Communication Research* 570.

5.62 In the case of *R v Woods,*[56] for example, the defendant, an unemployed 19-year-old, was convicted under section 127 of the CA 2003 for "jokes" he made on his Facebook page. The comments related to April Jones, a five-year-old from Machynlleth, Wales who was abducted and murdered, and Madeline McCann, a three-year-old who went missing from a hotel room in Portugal in 2007.[57] The comments made included:

> Who in their right mind would abduct a ginger kid?
>
> 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. April fools, who wants Maddie? I love April Jones.[58]

5.63 While Woods maintained that he intended his comments to be as a joke, noting that the comments were made "in one moment of drunken stupidity",[59] he pleaded guilty and was sentenced to 12 weeks in prison. The presiding magistrate justified the severity of the sentence as being based on the "seriousness of the offence, the public outrage that has been caused and we felt there was no other sentence this court could have passed which conveys to you the abhorrence that many in society feel this crime should receive".[60]

5.64 The level of the sentence was perceived as particularly concerning, given the fact that in other similar cases – such as that of *Thomas* – the Director of Public Prosecutions decided not to proceed with prosecution.

5.65 Thomas was a semi-professional footballer who posted a homophobic message on Twitter regarding Olympic divers Tom Daley and Peter Waterfield. The message came after they finished fourth in the 2012 Olympics, and read:

> If there is any consolation for finishing fourth at least daley and waterfield can go bum each other teamHIV[61]

---

56 S Morris and D Sabbagh, *April Jones: Matthew Woods jailed over explicit Facebook comments* (8 October 2012), available at https://www.theguardian.com/uk/2012/oct/08/april-jones-matthew-woods-jailed.

57 L Scaife, *Handbook of Social Media and the Law* (2015); see also R Griffiths, "Social media and the criminal law" (2013) 24(2) *Entertainment Law Review* 57, p 59.

58 L Scaife, *Handbook of Social Media and the Law* (2015); see also R Griffiths, "Social media and the criminal law" (2013) 24(2) *Entertainment Law Review* 57, p 59; and L Bliss, "The crown prosecution guidelines and grossly offensive comments: an analysis" (2017) 9(2) *Journal of Media Law* 173.

59 L Scaife, "The DPP and social media: a new approach coming out of the Woods?" (2013) 18(1) *Communications Law* 3, p 7.

60 L Scaife, *Handbook of Social Media and the Law* (2015) p 136.

61 J Valinsky, *Welsh soccer player under investigation for homophobic tweets about Tom Daley* (1 August 2012), available at https://www.dailydot.com/news/welsh-soccer-homophobic-tweets-tom-daley/.

5.66 The CPS in this case decided not to prosecute, noting that while the message was offensive, it was not grossly offensive and thus did not trigger criminal liability.[62] The DPP at the time, Keir Starmer QC, stated that it:

> was, in essence, a one-off offensive Twitter message, intended for family and friends, which made its way into the public domain. It was not intended to reach Mr Daley or Mr Waterfield, it was not part of a campaign, it was not intended to incite others and Mr Thomas removed it reasonably swiftly and has expressed remorse. Against that background, it was not so grossly offensive that criminal charges need to be brought.[63]

5.67 This announcement was in the lead up to the introduction of new CPS guidelines aiming to set a high threshold for prosecuting grossly offensive communication, with particular regard to the "spontaneous" use of social media and the right to freedom of speech.[64]

5.68 Concerns were raised over a seemingly inconsistent application of the notion of "gross offensiveness" to online communication.[65] The DPP commented on the difficulty in finding the line between merely offensive and grossly offensive as follows:

> … the CPS has the task of balancing the fundamental rights of free speech and the need to prosecute serious wrongdoing … That often involves very difficult judgment calls and, in the largely unchartered territory of social media, the CPS is prosecuting on a case by case basis. In some cases it is clear that a criminal prosecution is the appropriate response to conduct which is complained about… But in many other cases a criminal prosecution would not be the right response.[66]

5.69 These concerns led to the creation of the CPS guidelines for prosecuting cases involving communications sent via social media, referred to in Chapter 4. The guidelines state that prosecution for gross offensiveness under both the CA 2003 and MCA 1988 should only be commenced if the communication amounts to something that is *more than*:

(1) offensive, shocking or disturbing [comment]; or

(2) satirical, iconoclastic or rude comment; or

---

62 R Griffiths "Social media and the law" (2013) 24(2) *Entertainment Law Review* 57, p 58.

63 K Starmer QC, *DPP statement on Tom Daley case and social media prosecutions* (20 September 2012), available at http://blog.cps.gov.uk/2012/09/dpp-statement-on-tom-daley-case-and-social-media-prosecutions.html.

64 R Griffiths "Social media and the law" (2013) 24(2) *Entertainment Law Review* 57, p 59.

65 See, eg, L Bliss "The crown prosecution guidelines and grossly offensive comments: an analysis" (2017) 9(2) *Journal of Media Law* 177; J Rowbottom, "Crime and communication: do legal controls leave enough space for freedom of expression?" in D Mangan and L Gillies (eds) *The Legal Challenges of Social Media,* (2017) p 53.

66 K Starmer QC, *DPP statement on Tom Daley case and social media prosecutions* (20 September 2012), available at http://blog.cps.gov.uk/2012/09/dpp-statement-on-tom-daley-case-and-social-media-prosecutions.html.

(3) 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

(4) an uninhibited and ill thought out contribution to a casual conversation where participants expect a certain amount of repartee or "give and take"…. [67]

5.70 Drawing on case law, assessment is made by reference to:

> contemporary standards… the standards of an open and just multi-racial society, assessing whether the particular message in its particular context is beyond the pale of what is tolerable in society…

5.71 In the wake of cases such as *Woods* and *Thomas*, context is now regarded by the CPS to be highly important in determining whether or not material is "grossly offensive":

> Each case must be decided on its own facts and merits and with particular regard to the context of the message concerned. Context includes: who is the intended recipient? Does the message refer to their characteristics? Can the nature of the message be understood with reference to a news or historical event? Are terms which require interpretation, or explanation by the recipient, used? Was there other concurrent messaging in similar terms so that the suspect knowingly contributed to a barrage of such messages?[68]

5.72 Scaife has observed that:

> …prosecutors should have regard to the fact that the context in which interactive social media dialogue takes place is quite different to the context in which other communications take place…
>
> Banter, jokes and offensive comments are commonplace and often spontaneous.[69]

5.73 The stated intention of the CPS' guidelines is to "ensure that there is a consistency of approach across the CPS" with regard to the exercise of prosecutorial discretion.[70] However, since the guidelines were released, controversy over charging and prosecution decisions has continued, with limited clarification in law of how those decisions are made. Below we illustrate through a number of case examples the

---

67 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (last revised 21 August 2018), available at https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media.

68 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (last revised 21 August 2018), available at https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media.

69 L Scaife, *Handbook of Social Media and the Law* (2015) p 146.

70 See, eg *Full text: CPS Interim guidelines on prosecuting cases involving communications sent via social media* (19 December 2012), available at https://www.mirror.co.uk/news/uk-news/cps-interim-guidelines-prosecuting-cases-1496815.

inherent difficulty of the task facing prosecutors and courts in applying the "grossly offensive" standard.

Prosecuting gross offensiveness post-CPS guidelines

5.74 Precisely which factors are considered when determining whether a communication crosses the threshold from mere offensiveness to gross offensiveness, is still not clear in charging decisions nor in the case law. Racially aggravated statements and communications targeting specific high-profile figures appeared to amount for a significant proportion of prosecutions in the sample of cases between June 2016 and June 2018, from internal case management data provided by the CPS.[71]

5.75 An example which suggests some ongoing lack of clarity was the 2014, prosecution of Jordan Barrack, who pleaded guilty to posting "grossly offensive" images on social media under section 127 of the CA 2003. Barrack had posted on Snapchat and Facebook a photo of two police officers, on which he had drawn two penises. He had been waiting over two hours to be interviewed in relation to witnessing an incident at a bar.[72]

5.76 With limited reported cases to rely on, it is difficult to determine why the CPS decided that this particular case crossed the threshold from being "offensive, shocking or disturbing" to "grossly offensive". It may well have been that the fact the matter was targeted at a police officer that factored into the messages crossing the threshold of gross offensiveness. Whatever the reason, if "gross offensiveness" is to continue to be included in communications offences, the law may need to provide more clarity as to how it may be determined. 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.

5.77 A recent example where clearer tests may have proved helpful was a charge authorised by the CPS for two photos posted of body bags (one closed, one open) at the site of the Grenfell Tower disaster.[73] This decision has been criticised by human rights groups on the basis that it unreasonably infringes on freedom of expression.

---

71 Note that the CPS does not collect data that constitutes official statistics as defined in the Statistics and Registration Service Act 2007. These data have been drawn from the CPS's administrative IT system, which (as with any large scale recording system) is subject to possible errors with data entry and processing.

72 Mail Online, *Builder ordered to pay £400 after drawing two penises on a picture of him and posting it on Facebook* (5 February 2014), available at http://www.dailymail.co.uk/news/article-2552269/Builder-ordered-pay-policeman-400-drawing-two-penises-picture-posting-Facebook.html; and J Taylor, "British Man Fined $800 for Drawing Dicks On a Snapchat Picture of a Cop" (2 February 2014), available at http://observer.com/2014/02/british-man-fined-800-for-drawing-dicks-on-a-snapchat-picture-of-a-cop/.

73 J Nevett, *Bloke 'who posted Grenfell fire victim pic to Facebook' charged with criminal offence* (16 June 2017), available at https://www.dailystar.co.uk/news/latest-news/622764/man-arrested-grenfell-fire-victim-picture-facebook-criminal-offence; S Paterson, *Neighbour who opened Grenfell Tower body bag and posted pictures of dead victim on Facebook is jailed for three months* (16 June 2017), available at http://www.dailymail.co.uk/news/article-4611862/Man-jailed-posting-Grenfell-Tower-victim-picture.html; and S Jones, *Facebook ghoul who photographed dead Grenfell Tower fire victim in body bag is jailed for three months* (16 June 2017), available at https://www.mirror.co.uk/news/uk-news/facebook-ghoul-who-photographed-dead-10635450.

5.78 As we note in Chapter 9, section 127 of the CA 2003 and section 1 MCA 1988 are regularly used to prosecute hate speech. The most recent CPS hate crime annual report indicates that 7.2% of all prosecutions under these offences were flagged as hate crimes.[74]

5.79 In 2017, for example, Chelsea Russell was convicted for sending a grossly offensive message under section 127 of the CA 2003 after she posted on Instagram a lyric from Snap Dogg's rap song "I'm Trippin'' containing a racial term, in a tribute to a boy who died in a car crash.[75]

5.80 The CPS authorised the charge on the basis of "gross offensiveness". The magistrates' court sentenced her to an eight-week curfew and imposed an order for costs.[76] However, the message was quoting from a song that had been performed on stage in front of thousands of people, provoking controversy as to how her online communication could rightly be criminalised, when the equivalent offline communication is not.

5.81 Another case that sparked controversy was the case of Alison Chabloz, who was convicted of posting "grossly offensive" material onto YouTube by way of videos of antisemitic songs, written and performed by her, which mocked the Holocaust. The prosecution was initially brought privately by the charitable organisation Campaign Against Antisemitism, and later taken over by the CPS. One song was titled (((survivors))), a play on the online convention used by white supremacists who place Jewish names within three brackets. Lyrics of the songs included:

> Did the Holocaust ever happen? Was it just a bunch of lies? Seems that some intend to pull the wool over our eyes.[77]
>
> Now Auschwitz, holy temple, is a theme park just for fools, the gassing zone a proven hoax, indoctrination rules.[78]

5.82 While Chabloz defended her songs as satire, the magistrates were satisfied that they were grossly offensive and intended to offend Jewish people.[79]

5.83 These cases demonstrate the way in which section 127 of the CA 2003 is often used as a "catch all provision" for speech that is not caught by "substantive offences" such

---

74 Crown Prosecution Service, *Hate Crime Report 2017-18* (October 2018) p 18, available at https://www.cps.gov.uk/sites/default/files/documents/publications/cps-hate-crime-report-2018.pdf.

75 BBC News, *Woman guilty of 'racist' Snap Dogg rap lyric Instagram post* (19 April 2018), available at https://www.bbc.co.uk/news/uk-england-merseyside-43816921.

76 BBC News, *Woman guilty of 'racist' Snap Dogg rap lyric Instagram post* (19 April 2018), available at https://www.bbc.co.uk/news/uk-england-merseyside-43816921.

77 M Belam, *Woman who posted Holocaust denial songs to YouTube convicted* (25 May 2018), available at https://www.theguardian.com/uk-news/2018/may/25/woman-who-posted-holo'caust-denial-songs-to-youtube-convicted-alison-chabloz.

78 Campaign Against Antisemitism, *Alison Chabloz convicted on three charges over anitsemitic songs in landmark verdict, following private prosecution by CAA* (25 May 2018), available at https://antisemitism.uk/alison-chabloz-convicted-on-three-charges-over-antisemitic-songs-following-private-prosecution-by-caa/.

79 BBC News, *Alison Chabloz avoids jail over anti-Semitic songs* (14 June 2018), available at https://www.bbc.co.uk/news/uk-england-derbyshire-444846322.

as the "stirring up" offences in Parts III or IIIA of the Public Order Act 1986. It also suggests that the presence of racially offensive speech may be a key factor in determining whether a message is grossly offensive. However, these types of cases continue to create controversy, particularly in relation to context, which also suggests that further clarification – beyond the CPS guidelines – may be required to address some of the difficulties in applying the "grossly offensive" test.

5.84 Without further clarification in law there is a risk of overcriminalisation of online communication for gross offensiveness. This can tip the balance of parity between offline and online communication; with online communication being subject to a greater risk of prosecution for "gross offensiveness" than offline communication.

Gross offensiveness and the right to freedom of expression

5.85 Chapter 2 outlined the right to freedom of expression contained in Article 10 of the European Convention on Human Rights ("ECHR"), and the potential challenges in balancing the protection of this right with the need to regulate abusive and offensive online communication.

5.86 The question as to how far the law should go in prohibiting "grossly offensive" communication without unnecessarily inhibiting the right protected by Article 10 was raised in the Northern Irish case of *McConnell.*[80] In this case, the defendant was an evangelical Protestant preacher who severely criticised Islam in one of his sermons, which was transmitted on the internet and made into a DVD. The sermon contained the statement that "Islam is heathen, Islam is satanic, Islam is a doctrine spawned in hell". McConnell was charged under section 127 of the CA 2003. The District Judge, although accepting that the statement was "grossly offensive", ruled that it was protected by McConnell's rights under Articles 9 (freedom of thought, conscience and religion) and Article 10 of the ECHR.

5.87 It is worth nothing that the Indian Supreme Court ruled in *Shreya Singhal v Union of India*[81] that section 66A of the Information Technology Act – almost identical to section 127(1) of the CA 2003 – was incompatible with the right to free speech. The Court concluded that the section was unconstitutionally vague and "arbitrarily, excessively and disproportionately invades the right of free speech and upsets the balance between such right and the reasonable restrictions that could be imposed on such a right".[82]

5.88 It also found that the law was overreaching, including protected and innocent speech that meant it could have a "chilling effect" on free speech. After an analysis of the *Collins* case, the Court stated:

> 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

---

80 *DPP v James McConnell* [2016] NIMag 1.

81 (2015) Write Petition (Criminal) No 167 of 2012.

82 *Singhal v Union of India* (2015) Write Petition (Criminal) No 167 of 2012 at [82].

"menacing" are so vague that there is no manageable standard by which a person can be said to have committed an offence.[83]

5.89 The approach in England and Wales has differed greatly in maintaining that the provisions criminalising "gross offensiveness" are justified interferences with the right to freedom of expression. This must be carefully considered in light of the inconsistencies in prosecutions under section 127(1) of the CA 2003 and section 1 MCA 1988, to avoid the potential "chilling" effect on the right protected by Article 10.

CONCLUSION

5.90 This Chapter has reviewed the current case law and application of the notion of "gross offensiveness" in the context of communications offences.

5.91 The sending of "grossly offensive" messages is a crime that can be committed in the online world just as it can be in the offline world.

5.92 The definition of "gross offensiveness" in the law is still not clear. The case examples referred to throughout this Chapter demonstrate the difficulty in applying the term "gross offensiveness" to both offline and online communications. This suggests that the concept at law may be too vague and malleable, and further clarification may be required.

5.93 Further, the introduction of the internet and the rise of social media introduced more problems for the notion of gross offensiveness than perhaps was foreseen when section 1 of the MCA 1988 and even section 127 of the CA 2003 were enacted.

5.94 Online communications can create a permanent, searchable record, and be disseminated to a much wider audience than the sender originally intends, invariably much larger than any private offline communication. A communication on social media, for example, may be posted before the sender has had a chance to think through the consequences of their actions. The fact that people may engage with one-on-one, or one-on-many, communication at the touch of a button has transformed the landscape as it applies to gross offensiveness. As a result, the criminalisation of "grossly offensive" communications can capture a very wide array of online communication. Grossly offensive communication may in fact be more broadly criminalised online than in the offline world.

5.95 The CPS guidelines have attempted to deal with the malleability of the term "gross offensiveness", however, it is difficult to achieve clarity when the law itself is vague and unclear.

5.96 We therefore consider that any further review of the communications offences as they apply online should examine whether the offences relating to the sending of grossly offensive communications remain appropriate as a basis for criminal liability in England and Wales.

---

83 *Singhal v Union of India* (2015) Write Petition (Criminal) No 167 of 201 at [82].

Chapter 6: Obscenity and indecency

INTRODUCTION

6.1 The criminal law prohibits various forms of communicating obscene and indecent images, including possession of extreme pornography. A range of offences also apply in relation to the possession, production and dissemination of indecent images of children, but these offences are not within the remit of this Report.[1]

6.2 In an online world, obscene or indecent communication can occur via a conversation between two or more people (for example, over email, mobile, text, Facebook chat, WhatsApp or via an online chat room); or by sharing online (including sending images to one or more persons, posting on social media such as tweeting or a Facebook post, or creating a website).

6.3 This Chapter will review the laws relating to obscenity and indecency, particularly:

(1) the Obscene Publications Act 1959;

(2) the communications offences in section 127 of the Communications Act 2003 ("CA 2003") and section 1 of the Malicious Communications Act 1988 ("MCA 1988");

(3) the Indecent Displays (Control) Act 1981;

(4) the common law offences of "outraging public decency" and "conspiracy to corrupt public morals";

(5) the offence of exposure under section 66 of the Sexual Offences Act 2003; and

(6) the possession of "extreme pornography" under the Criminal Justice and Immigration Act 2008.[2]

6.4 The Chapter concludes with a variety of examples to illustrate the issues posed by the application and enforcement of laws regulating obscenity and indecency in the online environment.

---

1 This includes the Criminal Justice Act 1988, s 160 (possession of indecent photographs of children); the Protection of Children Act 1978, s 1 (making etc indecent photographs of children); the Children and Young Persons (Harmful Publications) Act 1955; and a number of offences under the Sexual Offences Act 2003, including sections 8 and 10 (causing or inciting a child to engage in sexual activity), section 12 (causing a child to watch a sexual act), section 14 (arranging or facilitating commission of a child sex offence) and section 15A (sexual communication with a child).

2 Note that offences relating to terrorist acts are not within the scope of this Report.

OBSCENE PUBLICATIONS ACT 1959

6.5 Section 2 of the Obscene Publications Act 1959 ("OPA 1959") provides that a person commits an offence if he or she:

> whether for gain or not, publishes an obscene article or … has an obscene article for publication for gain (whether gain to himself or gain to another).

6.6 Mere possession of an obscene article will not be a section 2 offence; it must be owned, possessed or within the person's control with a view to its publication for gain.

6.7 This creates two separate ways of committing the offence in section 2: publishing an obscene article, or "having" an obscene article for publication for gain (whether gain to the person possessing it, or to another). The latter offence was added by amendment by section 1(1) of the Obscene Publications Act 1964 ("OPA 1964").

6.8 According to section 1(2) of the OPA 1964, a person "shall be deemed to have an article for publication for gain if with a view to such publication he has the article in his *ownership, possession or control*" (emphasis added).

6.9 The meaning of "publish" for the purposes of the OPA 1959 is contained in section 2(3) and includes where a person:

> (a) distributes, circulates, sells, lets on hire, gives, or lends it, or … offers it for sale or for letting on hire; or
>
> (b) in the case of an article containing or embodying matter to be looked at or a record, shows, plays or projects it or, where the matter is data stored electronically, transmits that data.

6.10 There are challenges in defining the term "publish" in relation to online communication, which are discussed further below.

6.11 The intention of the author, including their honesty of purpose, is irrelevant to the determination of whether the article is obscene, as long as the effect of the article itself tends to deprave and corrupt those that are likely to read, see or hear it.[3]

6.12 Prosecutions for a section 2 offence require the consent of the Director of Public Prosecutions where the article in question "is a moving picture film of a width of not less than sixteen millimetres and the relevant publication … took place or (as the case may be) was to take place in the course of an exhibition of a film".[4] In a digital age, this safeguard may not have very wide application. As will be outlined further below, this is one of many aspects of the OPA 1959 that has not been adapted to the address the realities of the modern technological environment.

---

3 *Shaw v DPP* [1962] AC 220 at 227.

4 Obscene Publications Act 1959, s 2(3A).

6.13 The offence is punishable summarily by a fine or imprisonment (not exceeding six months), or, on indictment, by fine or imprisonment for up to five years.[5]

6.14 Section 2(3) of the Act contains a time limitation provision requiring commencement of the proceedings within two years from the date of commission of the offence. As discussed in Chapter 4, difficulties can arise in determining the date of commission of online offences. This may be particularly difficult to determine, where the possession (for gain) variant of the offence is charged.

6.15 Internal management data provided[6] by the Crown Prosecution Service ("CPS") show that 36 cases under the OPA 1959 made it to a first hearing in 2017, down from 45 in 2016.[7] However, only six convictions were entered under the OPA 1959 in 2016, down from 42 convictions in 2002.[8] The creation of the offences in section 127 of the CA 2003 and section 66 of the Criminal Justice and Immigration Act 2008 may partly explain this decrease. Both provisions also criminalise sending obscene messages, as will be outlined below.

Meaning of "obscenity"

6.16 The test for "obscenity" is contained in section 1(1) of the Act, which provides that an article is obscene when 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.

6.17 This definition of obscenity is derived from the "Hicklin principle". In the *Hicklin* case, Lord Cockburn CJ defined the term as where there was a tendency to "deprave and corrupt those whose minds are open to […] immoral influences and into whose hands a publication of this sort may fall".[9] This made it possible to treat a work as obscene, not on the basis of any intended readership, but rather on an assessment of the impact on, for example, children or other vulnerable groups whose minds are "open to immoral influence".

6.18 A key change in the OPA 1959 was to require explicit consideration of contextual information. Indeed, since the focus of this test is on those who are "likely" to read, see or hear the material, section 2 of the OPA 1959 has been termed a "context-dependent crime".[10]

---

5 Obscene Publications Act 1959, s 2(1).

6 Note that CPS does not collect data that constitutes official statistics as defined in the Statistics and Registration Service Act 2007. These data have been drawn from the CPS's administrative IT system, which (as with any large scale recording system) is subject to possible errors with data entry and processing.

7 It is noteworthy that the 2017 figure is still double the amount of cases that went to first hearing in 2015 (18).

8 J Rowbottom, "The transformation of obscenity law" (2018) 27(1) *Information & Communications Technology Law* 4, p 9.

9 *R v Hicklin* (1868) LR 3, QB 360, p 371.

10 J Jaconelli, "Context-Dependent Crime" [1995] *Criminal Law Review* 771.

6.19 Where the possession variant of the section 2 offence is prosecuted, section 1(3)(b) of the OPA 1964 states that:

> the question whether the article is obscene shall be determined by reference to such publication for gain of the article as in the circumstances it may reasonably be inferred he had in contemplation and to any further publication that could reasonably be expected to follow from it, but not to any other publication.

6.20 Therefore, the question of whether an article is obscene will depend on how, and in what context, the defendant intended to publish the article, which can be reasonably inferred from the evidence.

6.21 Obscenity under the OPA 1959 is an objective question, to be determined by the judge or jury relying on community standards, without the assistance of expert opinion.[11] A jury or magistrate must apply the standards of "ordinary, decent, right-minded people" in considering whether an article is obscene[12] and consider that these standards may change over time.

6.22 The standard for obscenity is distinct from indecency, as clarified in *R v Penguin Books*,[13] although the term indecency is not defined in law. Obscenity extends beyond sexual imagery. For example, in *John Calder (Publications) Ltd v Powell,*[14] which concerned a book about drug-taking, the Court held that the trial judges were entitled to find that particular material, unrelated to sex, was obscene.

6.23 According to the current CPS Guidance,[15] the types of material most commonly prosecuted under the OPA 1959 include:

(1) sexual acts with an animal;

(2) realistic portrayals of rape;

(3) sadomasochistic material "which goes beyond trifling and transient infliction of injury";

(4) torture with instruments;

(5) bondage;

(6) dismemberment or graphic mutilation;

---

11 As noted in *R v Anderson* [1972] 1 QB 304, p 313.

12 *R v Elliott* [1996] 1 Cr App R 432, p 436. The fact that there are other articles being published that are as obscene or worse than the article in question does not render that article acceptable; the jury must consider solely the article before them: D Ormerod and D Perry (eds), *Blackstone's Criminal Practice 2019,* para B18.8.

13 [1961] *Criminal Law Review* 176.

14 [1965] 1 QB 509.

15 Crown Prosecution Service, *Obscene Publications*, available at https://www.cps.gov.uk/legal-guidance/obscene-publications.

(7) activities involving perversion or degradation ("such as drinking urine, urination or vomiting on the body, or excretion or use of excreta"); and

(8) fisting.

6.24 The CPS Guidance also states that material that tends to induce violence has been prosecuted under the OPA 1959.[16]

6.25 This is a non-exhaustive list, and recent prosecutions show that most prosecutions under the OPA 1959 are related to fantasies or discussions relating to child sexual abuse.[17]

6.26 However, it should be noted that at the time of writing this Report, the CPS was in the process of public consultation on a proposed revision of its current legal guidance on obscene publications.[18] This consultation closed on 17 October 2018, and proposed to substantially amend the existing guidance. The proposed revisions are intended to provide more clarity about what an "obscene publication" might be, and to place an increased focus on those who may view this material, which may determine whether a criminal offence has been committed. The proposed revisions do not list the most common types of material prosecuted under the OPA 1959.

6.27 According to the existing CPS Guidance, the CPS would generally not advise proceedings in relation to actual consensual sexual intercourse, oral sex, masturbation, mild bondage, simulated intercourse or anal sex, or fetishes ("which do not encourage physical abuse") unless any of the aforementioned factors (listed in para 6.23) exist.[19] In contrast, the suggested revisions state that certain practices that are set out in current (at the time of writing) guidance, such as fisting, activity involving bodily substances, infliction of pain or torture, the use of bondage or restraint, placing objects into the urethra and any other sexual activity not prohibited by law, will not be likely to be prosecuted under the OPA 1959, provided that the activity is consensual, no serious harm is caused, it is not otherwise inextricably linked with other criminality, and the likely audience is not under 18 or otherwise vulnerable.[20]

---

16 Cases include *DPP v A & BC Chewing Gum Ltd* [1968] 1 QB 159; *John Calder (Publications) Ltd v Powell* [1965] 1 QB 509; *Calder and Boyars* Ltd [1969] 1 QB 151; and *Skirving* [1985] 1 QB 819.

17 Internal case management information provided by the CPS in relation to their review of the Obscene Publications Act 1959 showed that of the 32 prosecutions brought under section 2, between 1 January 2017 to 3 July 2018, 28 of those related to these communications (ie. by way of discussing with other adults their fantasies, intent to have, or actual experience of, sexual relations with children, or engaging in sexual conversations with children). Three prosecutions related to publications of bestiality.

18 See Crown Prosecution Service, *Obscene Publications – for consultation* (25 July 2018), available at https://www.cps.gov.uk/publication/obscene-publications-consultation. It was envisaged that the revised legal guidance would come into effect in late 2018.

19 Crown Prosecution Service, *Obscene Publications*, available at https://www.cps.gov.uk/legal-guidance/obscene-publications.

20 See Crown Prosecution Service, *Obscene Publications – for consultation* (25 July 2018), available at https://www.cps.gov.uk/publication/obscene-publications-consultation. It was envisaged that the revised legal guidance would come into effect in late 2018.

6.28 These changing interpretations of what acts would fall under the OPA 1959 can be contrasted with how the legislation was enforced in its early years of operation. This is partly a reflection of the fact that the definition of obscenity is not fixed, and varies with changes in society. Statistics show that consumption of pornography in the United Kingdom is widespread,[21] and as Murray notes:

> [i]t is clear that the UK has become a more permissive society in relation to indecency and obscenity in the fifty years that the Obscene Publications Act has been in force.[22]

6.29 Nevertheless, the Home Office and the Scottish government, in their joint consultation on the possession of extreme pornographic material in 2005, were satisfied that the concept of obscenity "continues to provide a benchmark for society's tolerance of certain material at a given time, as expressed through the courts".[23]

"Deprave and corrupt"

6.30 In the case of *R v Anderson,*[24] it was confirmed that "obscenity" under the OPA 1959 is not based on the same test as section 11 of the Postal Office Act 1953; that is, whether the matter is shocking, lewd or indecent. Rather, it is a question of whether the material has a tendency to "deprave and corrupt". [25]

6.31 "Deprave and corrupt" was defined in *Penguin Books*[26] (and approved in *R v Calder and Boyars Ltd*[27]*)* by Justice Byrne:

> …to deprave means to make morally bad, to pervert, to debase or to corrupt morally. To corrupt means to render morally unsound or rotten, to destroy the moral purity or chastity, to pervert or ruin a good quality, to debase, to defile.[28]

6.32 Further guidance was provided in *DPP v Whyte*,[29] where Lord Pearson noted that the words "deprave and corrupt" refer "to the effect of an article on the minds (including the emotions) of the persons who read or see it".[30] This includes, for example, stimulating fantasies and does not require overt physical or sexual activity to result from it.

---

21 See, eg J M Ruxton, *The most-watched porn of 2017 and the horniest countries* (10 January 2018), available at https://www.buzz.ie/life-style/watched-porn-2017-horniest-countries-268463.

22 A Murray, *Information Technology Law* (3rd ed, 2016) p 394.

23 Home Office and Scottish Executive, *Consultation: On the possession of extreme pornographic material* (August 2005) p 8, available at http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/30_08_05_porn_doc.pdf.

24 [1972] 1 QB 304.

25 *R v Anderson* [1972] 1 QB 304, p 312.

26 *R v Penguin Books* [1961] *Criminal Law Review* 176.

27 [1969] 1 QB 151.

28 *R v Penguin Books* [1961] *Criminal Law Review* 176*,* p 177.

29 [1972] AC 849.

30 [1972] AC 849, p 864.

6.33 The pool of people who are likely readers do not necessarily have to be "wholly innocent" but can include regular readers of obscene publications. In *Whyte*,[31] the Court noted that those who were already depraved and corrupt could be further depraved and corrupted. Lord Wilberforce emphasised that the intention of the legislation is equally to prevent the "less innocent" from further corruption, or feeding their addictions, as the "innocent" from initial corruption.[32]

6.34 No evidence is required of who exactly read or viewed the publication. A person does not need to have viewed or read the article, or have been depraved and corrupted by it, for an offence to have occurred under the OPA 1959.[33] The question is whether a person or a number of people were *likely* to see the article, and if so, whether the effect of the article as a whole was such as would deprave or corrupt those likely to have viewed or read it.[34]

6.35 There is no minimum number of likely readers required to pass the test for obscenity. However, case law initially suggested that of the likely readers, it is sufficient that the article tends to deprave or corrupt a "significant portion" of them.[35] There is no specified number as to what is "significant", however, it must not be "so small as to be negligible".[36]

Defences

6.36 The OPA 1959 provides two statutory defences.

6.37 Section 4(1) of the OPA 1959 provides a "public good" defence stating that an offence under section 2 will not be committed if it is proved that the publication is "justified as being for the public good on the ground that it is in the interests of science, literature, art or learning, or of other objects of general concern". For example, the defence could be triggered if an article was obscene but designed to discourage, rather than encourage, the behaviour depicted or described.[37]

6.38 Section 4(1)(A) provides a separate public good defence for moving picture films and soundtracks. It must be "proved that the publication of the film or soundtrack is justified as being for the public good on the ground that is in the interests of drama, opera, ballet or any other art, or of literature or learning".

---

31 *DPP v Whyte* [1972] AC 849.

32 *DPP v Whyte* [1972] AC 849, p 863.

33 *R v Perrin* [2002] EWCA Crim 747 at [22].

34 *R v Perrin* [2002] EWCA Crim 747 at [19].

35 *R v Calder and Boyars Ltd* [1969] 1 QB 151.

36 *DPP v Whyte* [1972] AC 849, p 865.

37 Noted by Salmon LJ in *R v Calder and Boyars Ltd* [1969] 1 QB 151 and approved in *R v Anderson* [1972] 1 QB 304; known as the "aversion argument".

6.39 Section 2(5) provides a defence if a defendant proves that they did not examine the article and "had no reasonable cause to suspect" that it was an obscene publication criminalised under the Act.[38]

Online challenges

6.40 There are a number of challenges in applying this obscenity test to online communications, including:

(1) the context-dependent nature of the offence;

(2) how online "articles" are defined, and how the obscenity test applies to them;

(3) the meaning of publication; and

(4) jurisdictional considerations.

6.41 These are explored further below.

Obscene publication as a context-dependent offence[39]

6.42 As noted above, the OPA 1959 requires consideration of the effect on likely readers of the material, rather than only those vulnerable to corruption. The offence requires consideration of the nature of the reader or viewer. Lord Wilberforce stated in *Whyte*[40] that:

> … to apply different tests to teenagers, members of men's clubs or men in various occupations or localities would be a matter of common sense.[41]

6.43 One of the major challenges posed by the internet is that it makes any content published online readily accessible to anyone with an internet-enabled device. Where material is made publicly available online, those that are likely to see or read it could include individuals of all ages, including "vulnerable young people", as was noted in *R v Perrin*.[42]

6.44 In 2006, the Government addressed the question of how the OPA 1959 applies to websites, in the context of a question about its use for child protection. Vernon Coaker MP, then Parliamentary Under Secretary for the Home Office, noted in this debate that the obscenity test in the OPA 1959 applies to:

> material which is not behind a suitable payment barrier or other accepted means of age verification, for example, material on the front page of pornography websites and

---

38 Obscene Publications Act 1959, s 2(5).

39 Term used in J Jaconelli, "Context-Dependent Crime" [1995] *Criminal Law Review* 771.

40 *DPP v Whyte* [1972] AC 849.

41 *DPP v Whyte* [1972] AC 849 at 863.

42 [2002] EWCA Crim 747 at [22].

non-commercial, user-generated material which is likely to be accessed by children and meets the threshold.[43]

6.45 This statement now appears out of line with the CPS charging policy as noted above, even if correct as a matter of legal principle. However, Part 3 of the Digital Economy Act 2017 – which creates, among other things, requirements to prevent access to pornographic material to persons under eighteen years of age – may impose financial penalties on those that fail to comply with these obligations.[44]

Online "articles" and obscenity

6.46 The offences in section 2 of the OPA 1959 relate to the publication, or possession with a view to publication, of an obscene "article".

6.47 "Article" is broadly defined in section 1(2) as "any description of article 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".

6.48 Communications over the internet, such as email, may constitute articles according to this definition. The email will contain matter (words, for example) to be read or looked at. Equally, videos, pictures or sound recordings shared over the internet are clearly within the definition. In *R v Waddon*,[45] for example, the defendant was prosecuted for eleven counts of publishing an obscene article on a website, namely computer images containing pornographic material.[46]

6.49 However, the complexity of the online environment can render these fundamental definitional issues difficult to apply in practice. *R v Smith*[47] involved a prosecution for sending obscene articles to another individual using "internet relay chat ("IRC")".[48] The chat logs were found on his computer and discussed explicit, incestuous and sadistic sexual acts on young children. Smith was charged with nine counts of publishing an obscene article contrary to section 2 of the OPA 1959. The "article" in each case was the comment or statement transmitted,[49] rather than the entire chat log of his comments, which were transmitted to the IRC servers and then to the other participant in the conversation.

---

43 *Hansard* (HC), 13 Dec 2006, vol 454, col 1122W.

44 Digital Economy Act 2017, s 20.

45 [2000] All ER (D) 502.

46 *R v Waddon* [2000] All ER (D) 502 at [1]. Waddon was also charged and convicted of one count of having an obscene article for publication for gain.

47 [2012] EWCA Crim 398; [2012] 1 WLR 3368.

48 Internet Relay Chat is "an open protocol that allows users with an IRC client to exchange text messages in real time over the internet". See Techopedia, *Internet Relay Chat (IRC)* (2018), available at https://www.techopedia.com/definition/403/internet-relay-chat-irc.

49 *R v Smith* [2012] EWCA Crim 398; [2012] 1 WLR 3368 at [8] and see also [22].

6.50 As Gillespie observes, treating the individual comments as separate "articles" raises the question of "whether, and when, those individual words become an article".[50] An electronic file containing all of the conversation and published online will clearly come within the definition of an article, as it would "contain" or "embody" matter to be read or looked at, but where words or statements are relied upon, "precisely what that article is can be difficult to capture".[51]

6.51 In *Smith*,[52] the Court of Appeal treated the comments as synonymous with "articles",[53] upheld the prosecution's appeal against a "terminatory" ruling in the Crown Court trial, and ordered a fresh trial.

6.52 The approach followed by the Court in *Smith*[54] appears difficult to reconcile with other aspects of the OPA 1959, in particular the definition of obscenity. Section 1 of the OPA 1959 differentiates between articles generally, and articles that "comprise … two or more distinct items". In the latter case, the obscenity test is applied to each item, considering if the effect is:

> if taken as a whole, 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.[55]

6.53 In *Anderson*,[56] which concerned the publication of a magazine, the trial was conducted on the basis that the entire magazine was considered as a whole, rather than separate items within the magazine in isolation. On appeal, this approach was found to be flawed. Lord Widgery CJ, giving the judgment of the Court, noted that:

> It is in our view quite clear from section 1 that where you have an article such as this comprising a number of distinct items, the proper view of obscenity under section 1 is to apply the test to the individual items in question. It is equally clear that if, when so applied, the test shows one item to be obscene that is enough to make the whole article obscene.[57]

6.54 This suggests that in relation to "offline" articles, words or specific news items in a print publication would not constitute separate "articles". Rather, the print publication (for example, a newspaper or magazine) itself is the "article" that must be published for the offence to be committed. However, specific items within it (such as comments made in

---

50 A Gillespie, "Obscene conversations, the internet and the criminal law" [2014] *Criminal Law Review* 350, p 354.

51 A Gillespie, "Obscene conversations, the internet and the criminal law" [2014] *Criminal Law Review* 350, p 354.

52 *R v Smith* [2012] EWCA Crim 398; [2012] 1 WLR 3368.

53 *R v Smith* [2012] EWCA Crim 398; [2012] 1 WLR 3368 at [22].

54 *R v Smith* [2012] EWCA Crim 398; [2012] 1 WLR 3368.

55 Obscene Publications Act 1959, s 1(1).

56 *R v Anderson* [1972] 1 QB 304.

57 *R v Anderson* [1972] 1 QB 304, p 312.

particular sections) will be considered separately for the purposes of applying the obscenity test and could render the entire article obscene.

6.55 The effect of the approach adopted in *Smith*,[58] however, which treated each individual comment or statement as a separate "article", could have unintended consequences. The Court essentially treated each separate message to the IRC server as a separate article that was "published". A possible lacuna created by this approach, as discussed by Gillespie, is where an individual types an obscene statement but each word is typed and sent separately. If these words are obscene only in sequence, but not in isolation, it may be that the offence is not committed.[59]

6.56 At the same time, the definition of an "article" could also be problematic if a broader approach is adopted. In *Perrin*,[60] the obscene article for which he was prosecuted (as the publisher) was a webpage. The Court of Appeal found that "[s]ection 1(2) defines "article" in a way that clearly embraces the web page with which we are concerned".[61] While this may be true, it can be contrasted with the approach in *Waddon*,[62] and may create difficulties in the context of more sophisticated websites.

6.57 For example, different people could operate subdomains of a website,[63] and websites can also cater for user-generated content. If the website is taken to be the "whole article", those operating the website could find that their entire site is found to be obscene due to the actions of users or those engaging with the website. There are, of course, a number of distinguishing features between those operating a website with user generated content, and those editing a magazine like in *Anderson*,[64] and website operators can also rely on a number of defences.[65]

6.58 What these examples show is that the language of the OPA 1959, which was obviously drafted with the analogue – rather than the digital – world in mind, clearly creates interpretative difficulties when transposed to this environment.

Meaning of "publication"

6.59 In the case of *Barker*,[66] Mr Justice Ashworth categorised the different forms of publication into three groups; the first (where a person "sells, lets on hire, gives or lends") relates to publication to an individual; the second, "distributes and circulates",

---

58 *R v Smith* [2012] EWCA Crim 398; [2012] 1 WLR 3368.

59 A Gillespie, "Obscene conversations, the internet and the criminal law" [2014] *Criminal Law Review* 350, p 354.

60 *R v Perrin* [2002] EWCA Crim 747.

61 *R v Perrin* [2002] EWCA Crim 747 at [16].

62 The individual (obscene) computer images were the focus of the charge, rather than the publication of the webpage: *R v Waddon* [2000] All ER (D) 502 at [1].

63 See, eg K Jensen, *How to Make Money with a Subdomain*, available at https://smallbusiness.chron.com/make-money-subdomain-23678.html.

64 *R v Anderson* [1972] 1 QB 304.

65 See, eg Electronic Commerce (EC Directive) Regulations 2002, reg 19; and Obscene Publications Act 1959, s 2(5).

66 *R v Barker* (1962) 46 Cr App R 227.

relates to publication to more than one person or on a wider scale; and the third, merely offering for sale or letting on hire, could also constitute a publication.[67]

6.60 In the offline world, publication could be committed by, for example, selling an obscene magazine or book in a shop ("sells"), handing out leaflets on the street ("distributes"), or leaving leaflets on the street ("circulates").

6.61 In the online context, publication is usually proven by showing that the defendant has transmitted the stored data. This form of publication was inserted in 1994,[68] and while "transmission" is not explicitly defined in the statute, it has been broadly interpreted by the courts in cases involving the online environment.

6.62 In *Waddon*,[69] the Court of Appeal found that the various interactions that occur between computers when content is uploaded to servers hosting websites, all involve the "transmission" of data.[70] This means that there will be a publication when an image is uploaded to a website, and a separate publication may be made when the image is downloaded from the website.[71]

6.63 Where data comprising an article (such as a film) are stored on a local device or in "cloud" storage, and then transmitted over the internet (such as on a website or over email) this will clearly constitute a publication under the Act.

6.64 An issue raised by the *Smith*[72] case is whether there can be a publication where an article is only communicated to one other person. A general understanding of "publication" implies a wider circulation. However, as noted above, the chat logs in *Smith*[73] were not published more widely than that. The comments and statements which formed the substance of the prosecution were made in a one-to-one conversation with an unknown party. The Court of Appeal concluded that "in our judgment, to publish an article to an individual is plainly to publish it within the meaning of the Act".[74] This suggests that the OPA 1959 could potentially apply to private online conversations.

6.65 Gillespie has suggested that the decision in *Smith* over-broadens the application of the OPA and argued that "the OPA 1959 was never intended to regulate private communications and there is no reason for it to stray into this area".[75] He points to the availability of section 127 of the CA 2003 as an alternative charge for such cases, which is designed to apply to communication rather than publication.

---

67 *R v Barker* (1962) 46 Cr App R 227 at 230.

68 Criminal Justice and Public Order Act 1994, s 168(1), sch 9 para 3.

69 *R v Waddon* [2000] All ER (D) 502.

70 *R v Waddon* [2000] All ER (D) 502 at [19].

71 *R v Waddon* [2000] All ER (D) 502 [12].

72 *R v Smith* [2012] EWCA Crim 398; [2012] 1 WLR 3368.

73 *R v Smith* [2012] EWCA Crim 398; [2012] 1 WLR 3368.

74 *R v Smith* [2012] EWCA Crim 398; [2012] 1 WLR 3368 at [21].

75 A Gillespie, "Obscene conversations, the internet and the criminal law" [2014] *Criminal Law Review* 350, p 363.

6.66 However, while this point about the potential breadth of the OPA 1959 after *Smith*[76] is compelling, it does not necessarily follow that section 127 of the CA 2003 is an appropriate charge for some of the more serious offences under section 2 of the OPA 1959. For example, if someone live streams a rape or physical mutilation of someone for another person, section 127 of the CA 2003 may not be deemed to be an appropriate charge, as it carries a significantly lower maximum penalty (six months' imprisonment, rather than five years under the OPA 1959). A charge of possession of extreme pornography under section 66 of the CJIA 2008, detailed below, may also be available for this conduct.

6.67 This uncertainty again points to the need to reconsider how obscenity and indecency offences, such as those contained in the OPA 1959, should apply in the online environment.

Jurisdictional challenges

6.68 The "borderless nature"[77] of the internet presents challenges for policing and prosecuting obscene publications in an online context. A 2013 survey found that approximately 7% of global "adult content"[78] is hosted in the United Kingdom, which suggests that a significant amount of material that could be prosecuted under the OPA 1959, is in fact not sourced from England or Wales.[79]

6.69 The current CPS guidance on obscenity notes that "most publishers are outside the jurisdiction and cannot be prosecuted".[80] However, the criminal law does allow for cases with an extraterritorial dimension to be prosecuted.

6.70 The decisions of the Court of Appeal in *Waddon*[81] and *Perrin*[82] both interpret the jurisdictional ambit of the offences in the OPA 1959 very broadly in the context of publications over the internet.

6.71 In both cases, the defendants admitted responsibility for the relevant publication, but there was a crucial difference between them. In *Waddon*,[83] the uploading of the material occurred in this jurisdiction. In contrast, in *Perrin*,[84] it appears to have been argued that the French citizen, resident in London, had performed all material acts outside of the

---

76 *R v Smith* [2012] EWCA Crim 398; [2012] 1 WLR 3368.

77 A Murray, *Information Technology Law: The Law and Society* (2016) p 391.

78 Content designed for viewing by people 18 years or over, such as pornographic material.

79 D Holmes "Infographic: What Countries Host the Most Porn?" cited in A Murray, *Information Technology Law: The Law and Society* (2016) p 396.

80 Crown Prosecution Service, *Obscene Publications*, available at https://www.cps.gov.uk/legal-guidance/obscene-publications.

81 *R v Waddon* [2000] All ER (D) 502.

82 *R v Perrin* [2002] EWCA Crim 747.

83 *R v Waddon* [2000] All ER (D) 502 at [10].

84 *R v Perrin* [2002] EWCA Crim 747 at [4].

jurisdiction. There was, in any event, "no evidence as to where the data files were created and posted, and there was no evidence as to the location of the server".[85]

6.72 In the case of *Waddon*,[86] Lord Justice Rose concluded that where a defendant uploads stored data to a website, hosted abroad, there will be a publication both where the data is transmitted from England and Wales, as well as further publication where the data is transmitted back to this country when the website is accessed by someone here.

6.73 This approach was also accepted in the case of *Perrin*.[87] The "type" of "publication" relied on in the case was the "making available of preview material to any viewer who may choose to access it…".[88] Transmission of data in section 1(3)(b) can therefore occur anywhere in the world, and on the approach adopted in *Perrin*, once the material is "available" within the jurisdiction, the offence occurs here.

6.74 Hirst criticises the decision in *Perrin* and contends that a major error occurred in the Court's reliance on *Waddon*.[89] The latter case, he contends, was based on the "terminatory theory" (if the act affects a citizen within the territory of a state, discussed further in Chapter 2), because "the occurrence of a relevant transmission within the jurisdiction could not realistically be disputed",[90] as the preparation and uploading of the material occurred in England. Where mere accessibility of content suffices to constitute a domestic publication, this generates the problems of jurisdictional concurrency explained in Chapter 2, as a person could potentially be liable in every jurisdiction with internet connectivity if other countries adopted a similar approach in their domestic obscenity laws.

6.75 It is also noteworthy that the Court of Appeal in *Perrin* "reject[ed] the suggestion that it is ever necessary for the [prosecution] to show where the major steps in relation to publication were taken".[91] This may need to be revisited in light of the developments in *Smith*[92] and *Sheppard*[93] (the latter of which endorsed the substantial measure test in the context of section 19 of the Public Order Act 1986).

6.76 However, the decision in *Perrin* simply highlights that on either approach towards territorial jurisdiction, the criminal law is far-reaching. The traditionally conservative terminatory theory was found to be sufficiently flexible to cover situations where the only domestic nexus involved accessibility of content, while the substantial measure test has been noted in Chapter 2 to be a malleable tool which could cover a similar situation, particularly if there is a targeting of the public in England and Wales.

---

85 *R v Perrin* [2002] EWCA Crim 747 at [33].

86 *R v Waddon* [2000] All ER (D) 502 at [10] and [12].

87 *R v Perrin* [2002] EWCA Crim 747 at [18].

88 *R v Perrin* [2002] EWCA Crim 747 at [22].

89 *R v Waddon* [2000] All ER (D) 502.

90 M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003) p 189.

91 *R v Perrin* [2002] EWCA Crim 747 at [52].

92 [2012] EWCA Crim 398; [2012] 1 WLR 3368.

93 [2010] EWCA Crim 65, [2010] 1 WLR 2779.

OBSCENITY AND INDECENCY IN THE COMMUNICATIONS OFFENCES

6.77 The communications offences are discussed in more detail in Chapter 4.

6.78 The offence under section 127(1)(a) of the CA 2003 includes sending by means of a public electronic communications network a message or matter that is of an "indecent" or "obscene" character.

6.79 The offence in section 1 of the MCA 1988 can also be committed by sending, for example, an electronic communication which conveys a message which is indecent, or an article or electronic communication which is, in whole or part, of an indecent nature.

6.80 The precise meaning of the terms "indecent" or "obscene" are unclear in the context of these communication offences, and is left to the jury to decide as a question of fact. Parliament thought it appropriate to leave it to the discretion of the courts, however, the courts have been reluctant to define "indecency" beyond it being a question of fact for the jury or magistrates based on reasonable standards.

6.81 In the Divisional Court in *Collins*, which concerned section 127 of the CA 2003, Lord Justice Sedley stated that both "indecency" and "obscenity" are "generally in the eye of the beholder; but the law has historically treated them as a matter of objective fact to be determined by contemporary standards of decency".[94]

6.82 In our report on poison pen letters, we adopted a similar position.[95] There is also support for this approach in the context of some of the postal offences which criminalised the sending of "indecent" and "obscene" "postal packets". In *Stanley*,[96] the Court of Appeal observed how "[t]he words ''indecent or obscene'' convey one idea, namely, offending against the recognised standards of propriety, indecent being at the lower end of the scale and obscene at the upper end of the scale."[97] It also said that the jury should adopt the standards of "ordinary right-thinking members of the public".[98] Given the historical legacy of the offence in section 127 of the CA 2003 discussed in Chapter 4, it is likely that such non-binding comment of the court will be relevant to determinations involving it.

6.83 However, case law has failed to delineate precisely where the boundary lies between "indecency" and "obscenity", including what the terms actually mean, beyond these

---

94 *DPP v Collins* [2005] EWHC 1308 (Admin) at [10]. The decision of the Divisional Court was reversed by the House of Lords, but this aspect of the Sedley LJ's judgment was not in issue or commented upon.

95 "Whether or not something is indecent will be judged by an objective standard and magistrates have to decide what are the 'recognised standards of propriety' and whether the contents in the particular circumstances of the case offend against those standards. Where terms such as "indecent" are used in statutory offences there is obviously some scope for magistrates (or juries, as the case may be) to bring their own judgment to bear in deciding whether or not something is of that character, but in view of the requirement of proof of a purpose to cause anxiety or we see no basis for objection on that ground": Poison Pen Letters (1985) Law Com No 147, para 4.17. Note that this fault element requirement is not present in the context of the Communications Act 2003, s 127.

96 *R v Stanley* [1965] 2 QB 327.

97 *R v Stanley* [1965] 2 QB 327, p 333.

98 *R v Stanley* [1965] 2 QB 327, p 333.

generalisations. In *Anderson*, for example, Lord Widgery CJ stated for the Court that in respect of the offence in section 11 of the Post Office Act 1953:

> obscene in its context as an alternative to indecent has its ordinary or as it is sometimes called dictionary meaning. It includes things which are shocking and lewd and indecent and so on.[99]

6.84 This appears to attempt to distinguish between obscenity and indecency, but then includes items that are indecent in the explanation of obscenity. In our report on poison pen letters, we also noted an overlap between the meaning of "indecency" and "gross offensiveness".[100]

6.85 The element of "indecency" in the context of child sexual abuse images can be satisfied by nakedness depending on the context,[101] but as Gillespie notes, "the harm caused to a child in the production of these images justifies the use of a lower threshold".[102] However, there is less certainty as to whether a naked photo of an adult can be considered indecent, and thus illegal under section 127 of the CA 2003.

6.86 Given the vagueness of the term "indecent", and the absence of definition – or even guidance – in case law, the term could potentially cover photos of naked adults, certainly if in sexualised poses. Given there is no consent element to the offence, on another interpretation, a consensual naked photo sent between two adults could be criminal.

6.87 The criminalisation of these images may not be justified. Gillespie therefore questions whether "indecency" is an appropriate threshold in broader communication offences:

> … the CA 2003 applies to a much broader range of material, including text and sound, and this must raise concerns about whether "indecent" is an appropriate threshold. The meaning of indecent must mean that virtually any sexualised conversation could be captured by this offence, even that between consenting adults—something that would seem on the face of it extraordinary.[103]

INDECENT DISPLAYS (CONTROL) ACT 1981

6.88 Section 1(1) of the Indecent Displays (Control) Act 1981 ("IDCA 1981") states:

---

99 *R v Anderson* [1972] 1 QB 304, p 311 to 312.

100 Poison Pen Letters (1985) Law Com No 147, para 4.17.

101 For example, Criminal Justice Act 1988, s 160 and Protection of Children Act 1978, s 1. The arrest of Julia Somerville and her partner Jeremy Dixon demonstrates how potentially "innocent" photos could be caught within this wide standard. See, eg R Fowler, *Julia Somerville defends 'innocent family photos'* (5 November 1995), available at https://www.independent.co.uk/news/julia-somerville-defends-innocent-family-photos-1538516.html.

102 A Gillespie, "Obscene conversations, the internet and the criminal law" [2014] *Criminal Law Review* 350, p 359.

103 A Gillespie, "Obscene conversations, the internet and the criminal law" [2014] *Criminal Law Review* 350, p 359.

> If any indecent matter is publicly displayed the person making the display and any person causing or permitting the display to be made shall be guilty of an offence.

6.89 The Act repealed earlier statutory offences relating to indecent material such as offensive (including indecent, obscene or profane) exhibitions under the Vagrancy Act 1824 and 1838 and the Indecent Advertisement Acts 1889.[104]

6.90 The offence is triable either way, with a maximum penalty of two years' imprisonment and/or an unlimited fine on indictment, or an unlimited fine if prosecuted summarily.[105]

6.91 Exceptions are contained in section 1(4) of the IDCA 1981 and include where the matter is displayed in a television broadcasting or programming service; in an art gallery or museum (and only visible from within); "displayed by or with the authority of, and visible only from within a building occupied by, the Crown or a local authority"'; or in a film, performance of a play or film exhibition.

6.92 The intention of the IDCA 1981 was to reduce the public display of sexually explicit magazines.[106]

6.93 However, there is no definition of "indecent" in the legislation, and no additional clarification has been provided. The lack of definition was challenged during the passing of the Act. For example, Michael McNair-Wilson MP said in a House of Commons debate in 1973:

> We also seem to believe that while we know what is obscene because we have passed legislation on it, we cannot define what is indecent. Yet we accept that there is such a thing as indecent display material. This is something of a paradox, if not illogical … How can we honestly say we can tell what is obscene but not what is indecent? … we should seek to define indecency in this context if we believe that we can define obscenity, simply because there is an illogicality about being able to describe the one without the other.[107]

6.94 In opposition, Edward Gardner MP said that the term:

> is a good, plain, well understood word that has a long legislative history. Going back through the statutes of the nineteenth century, which were aimed at the kind of offences with which we are concerned now, time and again the word "indecent" appears without any definition at all. The difficulty arises when one comes to define words of this kind, when one tries to provide a definition of, for example, obscenity, that will make sense in a court. It is almost an impossible thing to do.[108]

---

104 Discussed in M Childs, "Outraging public decency: the offence of offensiveness" [1991] *Public Law* 20.

105 Indecent Displays (Control) Act 1981, s 4(1).

106 M Childs, "Outraging public decency: the offence of offensiveness" [1991] *Public Law* 20.

107 *Hansard* (HC), 13 November 1973, vol 864, col 418.

108 *Hansard* (HC), 13 November 1973, vol 864, col 398.

6.95 The House decided it was not appropriate to define "indecent" for purposes of the IDCA 1981. The term has remained undefined in both statute and at common law.

6.96 Internal case management data provided by the CPS indicates that there have been no prosecutions under the IDCA 1981 since 2015. Prior to this, just one charge was authorised under the Act in each of 2014 and 2015.[109]

6.97 In 2014, a charge was authorised under the Act where the suspect was found by an off-duty police officer to be attaching images of a naked female to lamp posts. The original photographs were found at his home address; police suspected the images depicted his former partner.

6.98 In 2015, one charge under the Act was made where a suspect used an iPad on display in a Tesco store to take a picture of an indecent image (a pornographic image showing male and female genitalia) from his phone, and left the iPad on display.

6.99 There have been no reported charges under the IDCA 1981 for displaying an indecent image online. The likely charge in this context will usually be one of the communications offences, or the OPA 1959. However, if online platforms and websites could be considered public places, which is explored further below, then online displays of indecent material could also be prosecuted under this Act.

Meaning of a "public place"

6.100 A matter[110] is publicly displayed when it is "displayed in or so as to be visible from any public place".[111]

6.101 Section 1(3) of the IDCA defines "public place" as follows:

> any place to which the public have or are permitted to have access (whether on payment or otherwise) while that matter is displayed except:
>
> (a) a place to which the public are permitted to have access only on payment which is or includes payment for that display; or
>
> (b) a shop or any part of a shop to which the public can only gain access by passing beyond an adequate warning notice.

6.102 The above exceptions, however, "shall only apply where persons under the age of 18 years are not permitted to enter while the display in question is continuing".

---

109 Note that the CPS does not collect data that constitutes official statistics as defined in the Statistics and Registration Service Act 2007. These data have been drawn from the CPS's administrative IT system, which (as with any large-scale recording system) is subject to possible errors with data entry and processing.

110 Defined in Indecent Displays (Control) Act 1981, s 1(5).

111 Indecent Displays (Control) Act 1981, s 1(2).

6.103 Therefore, owners of sex shops selling indecent magazines or similar will not commit an offence if the public can only gain access by passing beyond an adequate warning notice, and persons under the age of 18 are not permitted to do so.[112]

6.104 A "warning notice" must comply with the requirements outlined in section 1(6) of the IDCA 1981. The equivalent protection in an online context may be where there is a paid website containing indecent material, which contains a warning notice (with the words in section 1(6)) that you must click to accept before entering the site, confirming your date of birth in the process.

6.105 Walden has argued that there is "nothing in the definition of 'public place' that restricts its applicability to physical locations, rather than cyberspace".[113] This would therefore appear to be another broad offence that could apply to any online public display of indecent matter, such as on a website or social media platform. However, the courts are yet to determine whether the online environment is a public place, and in some cases suggested it may not be, as discussed in paragraph 6.120 onwards below.

OUTRAGING PUBLIC DECENCY

6.106 Throughout history, the common law has recognised and criminalised a number of different forms of conduct that were said to outrage public decency.

6.107 The common law offence of outraging public decency has been used in relation to acts such as indecent exposure,[114] acts of lewdness involving sexual activity,[115] urinating on a war memorial while intoxicated,[116] physically abusing and urinating on a woman dying in the street,[117] upskirting[118] and simulations of sexual actions in front of boys.[119]

6.108 The question of whether an act has outraged public decency is a question for the jury,[120] similar to the finding of whether an article is obscene for the purposes of the OPA 1959.

6.109 The offence has developed as one of strict liability, emphasised by the Court of Appeal in *R v Gibson,*[121] which concerned an offensive display of a work of art, consisting of earrings made out of a human foetus.[122] While a defendant must be aware of the nature

---

112 Indecent Displays (Control) Act 1981, s 1(3)(b).

113 I Walden, *Computer Crimes and Digital Investigations* (2nd ed, 2016) at 3.148.

114 For example, ***Sedley's case*** [1714] EngR 392; more recently, *R v Walker (Steven)* [1996] 1 Cr App R 111.

115 For example, *R v Bunyan* (1844) 1 Cox CC 74*;* and *R v Mayling* [1963] 1 All ER 687; [1963] 2 WLR 709.

116 See, eg *R v Laing* (2009, unreported), available at http://www.theguardian.com/uk/2009/nov/26/student-urinated-war-memorial-sentenced.

117 See, eg *R v Anderson* [2005] EWCA Crim 3, [2008] 2 Cr App R (S) 57.

118 See, eg *R v Hamilton* [2007] EWCA Crim 2062, [2008] QB 224.

119 See, eg *R v May* (1989) 91 Cr App R 157, [1990] *Criminal Law Review* 415.

120 Judge Smedley said this to the jury in the initial trial of *R v Gibson*, and no fault was found on appeal with the summing up. Also emphasised in *R v Mayling* [1963] 2 QB 717.

121 [1990] 2 QB 619.

122 Co-defendants Gibson, who was an artist, and Sylverie, an art gallery operator, had displayed in Sylverie's gallery a model head with earrings made out of a freeze-dried human foetus.

of the act they are committing, they do not need to have necessarily intended to outrage public decency nor be aware but reckless of the risk of doing so.[123]

6.110 In our 2015 report on the offence, we recommended that the common law offence should be entrenched in statute, and include a fault element as well as a defence of reasonableness.[124]

6.111 Although there are no known reported cases of outraging public decency offences carried out online, the offence does not necessarily exclude online acts. The next section considers whether an online "act" could be considered to be "public" for the purposes of the offence, and whether minimum standards of decency are the same both online and offline.

6.112 The external elements of the offence were described by Lord Lane CJ in *May*[125] as follows:

> There must have been proved to have been an act of such a lewd, obscene or disgusting nature as to amount to an outrage on public decency.[126]

6.113 The conduct itself must be of a lewd, obscene or disgusting nature and cannot be inferred by intention or motive if the conduct itself lacks those qualities.[127]

6.114 There is no requirement for anyone to be actually disgusted or outraged for an offence to have been committed.[128]

6.115 The offence of outraging public decency is not focused on whether conduct tends to deprave and corrupt, as required under the OPA 1959, but rather the nature of the conduct (or, in the case of *Gibson,* article exhibited) being disgusting or offensive.[129]

6.116 The narrow distinction between these definitions could mean that the offence of outraging public decency may be applied to acts committed online that fall outside the OPA 1959.

6.117 Lord Reid defined "indecency" as "not confined to sexual indecency: indeed, it is difficult to find any limit short of saying that it includes anything which an ordinary man or woman would find shocking, disgusting or revolting".[130]

---

123 *R v Gibson* [1990] 2 QB 619; also discussed in T Rees, "Outraging public decency – whether prosecution for common law offence ousted by Obscene Publications Act 1959 – mens rea for common law offence" [1990] *Criminal Law Review* 738.

124 Simplification of Criminal Law: Public Nuisance and Outraging Public Decency (2015) Law Com No 358, p 73. Note there was no Government response to this report.

125 *R v May* (1989) 91 Cr App R 157.

126 *R v May* (1989) 91 Cr App R 157 at 159.

127 *R v Rowley* [1991] 1 WLR 1020.

128 *R v May* (1989) 91 Cr App R 157; see also *R v Mayling* [1963] 2 QB 717; *R v Choi* [1999] EWCA Crim 1279.

129 *R v Gibson* [1990] 2 QB 619.

130 *Knuller (Publishing, Printing and Promotions) Ltd v DPP* [1973] AC 435 at 458.

6.118 Lord Simon in this case described the word "outrage" as a strong term that goes "beyond offending the sensibilities of, or even shocking, reasonable people"[131] and should be based on "recognised minimum standards of decency, which are likely to vary from time to time".[132]

6.119 The question then is, could online acts that tend to "engender revulsion or disgust or outrage" be prosecuted as outraging public decency in the same way as similar offline acts? This may depend on how the notion of "public" is defined in relation to online communication. We discuss this further below.

Meaning of "public" and the online world

6.120 Whether or not an act is "public" for the purposes of this offence relates to its visibility. An act is "public" if more than one person is present and could have seen the act.[133]

6.121 The act does not necessarily have to be on public property or an open place so long as these two elements are satisfied.[134]

6.122 Whether or not an act was "public" for the purposes of the offence was considered in *Rose v DPP*.[135] In this case, the defendant was caught on CCTV exposing his genitals with a female who was performing oral sex on him in the foyer of a bank containing Automatic Teller Machines. The foyer was open and accessible to the public. No-one else was physically present at the time the defendant committed the act, however, it was seen on recorded CCTV footage by the manager of the bank the following day. Rose was charged with the offence of outraging public decency.

6.123 The issue in this case was whether the act was done in public, as it was only witnessed on a private CCTV system. The Court held that no common law offence of outraging public decency is committed if the act is not seen by anyone else not participating in it, noting that "the only evidence of anyone seeing this act was of one person seeing it, and, on the authorities… that is not a sufficient public element for the offence to be established."[136]

6.124 However, this is not to say that if more than one person had seen the CCTV footage, an offence of outraging public decency would not have been committed. The Court did not answer the question whether, if more than one person was present for the CCTV viewing – and not in the physical place at the time of commission – this would be sufficient to satisfy the public element of the offence. However, it was suggested that

---

131 *Knuller (Publishing, Printing and Promotions) Ltd v DPP* [1973] AC 435 at 495.

132 *Knuller (Publishing, Printing and Promotions) Ltd v DPP* [1973] AC 435 at 495. This case also confirmed the existence of the common law offence conspiracy to corrupt public morals, which is now entrenched in section 5(3)(a) of the Criminal Law Act 1977.

133 *R v May* (1989) 91 Cr App R 157; see also M Childs, "Outraging public decency: the offence of offensiveness" [1991] *Public Law* 20. In *R v Hamilton* [2007] EWCA 852; [2008] QB 224, the Court noted that although no one noticed the up-skirting act at the particular point in time, it was enough that at least two people *could* have noticed.

134 *R v Wellard* (1884-85) LR 14 QBD 6.

135 [2006] EWHC 852 (Admin); [2006] 1 WLR 2626.

136 *Rose v DPP* [2006] EWHC 852 (Admin); [2006] 1 WLR 2626 at [28].

physical presence in the same place at the time of commission may be required. Mr Justice Burnton said in a non-binding comment:

> There is, I think, considerable force in Mr Weatherby's submission that the viewing privately of a private recording of an act which had not previously been seen by any person is insufficient to constitute the offence. That is because the offence is committed when it is committed. It would be curious if the offence was completed by a private viewing of a recording and if it could make a difference, for example, as to whether the bank manageress was in the company of somebody else when she saw the video or not, or whether she showed it to someone else afterwards or not.[137]

6.125 This has potential implications for whether an act of outraging public decency could be committed in the online world. The courts have previously envisaged people being "present" for the purposes of the public element of the offence,[138] and this would have traditionally meant physical presence. Where the actual act occurs in the offline world but is live streamed or posted online, the physical act itself may constitute the offence. However, it remains to be decided whether, if more than one person can view such an act online, they are "present" for purposes of the common law offence.

6.126 The judgment in *Rose v DPP*[139] seems to suggest that if no one was physically capable of seeing the act at that physical place at the time of its commission, the offence of outraging public decency has not been committed. However, it leaves it open to suggestion as to whether the viewing of the act online, by more than one person, would satisfy the public element of the offence.

6.127 In *R v Hamilton,* the "public" element of the offence was clarified:[140]

> The public element in the offence is satisfied if the act is done where persons are present and the nature of what is being done is capable of being seen; the principle is that the public are to be protected from lewd, obscene or disgusting acts which are of a nature that outrages public decency and which are capable of being seen in public.[141]

6.128 However, this does not provide any further clarification as to whether, if persons are present "online" at the time of viewing, that this would satisfy the public element of the common law offence.

6.129 There may be a distinction between an act that was recorded and then posted online (where the viewers are seeing the act after it was actually committed, which may well not be an offence of outraging public decency) and if the act was live-streamed (where the viewers are witnessing the act in real time, albeit over the internet and not physically in the same place). It is possible that the latter scenario could constitute an offence of public decency, if there is more than one witness of the act at the time of commission.

---

137 *Rose v DPP* [2006] EWHC 852 (Admin); [2006] 1 WLR 2626 at [29].

138 *R v Hamilton* [2007] EWCA Crim 2062; [2008] QB 224 at [21].

139 [2006] EWHC 852 (Admin); [2006] 1 WLR 2626.

140 *R v Hamilton* [2007] EWCA 852; [2008] QB 224.

141 *R v Hamilton* [2007] EWCA 852; [2008] QB 224 at [21].

However, given that there can be very short time delays between an act in "real time" and its subsequent posting online (sometimes a matter of seconds), the former may still amount to an offence of outraging public decency, although this question is yet to come before the courts.

6.130 Courts in England and Wales have not yet ruled on whether the online environment could constitute a public place for the purposes of the outraging public decency offence, but this has been considered in other jurisdictions.

6.131 For example, Hong Kong's Court of Final Appeal decided in *Chan Yau Hei*[142] that the "internet"[143] was *not* a public place for purposes of the common law offence of outraging public decency, which required a specifically public locality.[144] The appellant had posted on an internet discussion forum called HK Golden the following message:

> We have to learn from the Jewish people and bomb the Liaison Office of the Central People's Government fire

6.132 The appellant had argued that:

> the internet discussion forum was not an act done in a place to which the public had access or where what was done was capable of public view and in a way which was capable of being seen or two or more persons who were actually present …[145]

6.133 It was not, therefore, of such a character as to outrage public decency.

6.134 This argument was initially rejected, and the appeal was dismissed at the first instance. The Court of Final Appeal, however, concluded that "the public element of the offence requires the act to be committed in a physical, tangible place".[146] It noted that all previous convictions for outraging public decency had occurred in physical, tangible places.

6.135 The Court of Final Appeal was of the view that "it is a fiction to describe the internet as a place in any physical or actual sense",[147] because the data uploaded to the internet "is simply computer code and is commonly described as being in "cyberspace" or in a "virtual" place or forum".[148] It is only when people download or access that translated code, from the computer in their living room (for example) that a person is outraged, in

---

142 *HKSAR v Chan Yau Hei* [2014] HKCFA 18; (2014) 17 HKCFAR 110.

143 This was the term that was used in the judgment, though the more pertinent question was whether the online "places" facilitated by the internet could come within the terms of the offence.

144 In *HKSAR v Chan Yau Hei* [2014] HKCFA 18; (2014) 17 HKCFAR 110, it was concluded that although the content of the message was capable of outraging public decency, the "public" element of the offence could not be satisfied because it was committed online and not in a public place. See also G Kennedy, "Hong Kong: Court of Final Appeal rules internet not to be a public place" (2014) 30(4) *Computer Law & Security Review* 456.

145 *HKSAR v Chan Yau Hei* [2014] HKCFA 18; (2014) 17 HKCFAR 110 at [10].

146 *HKSAR v Chan Yau Hei* [2014] HKCFA 18; (2014) 17 HKCFAR 110 at [37].

147 *HKSAR v Chan Yau Hei* [2014] HKCFA 18; (2014) 17 HKCFAR 110 at [45].

148 *HKSAR v Chan Yau Hei* [2014] HKCFA 18; (2014) 17 HKCFAR 110 at [45].

that “actual” place. The notion of being outraged is experienced in the physical world, not the virtual. Justice Fok PJ concluded:

> To hold that the internet is a public place for the purposes of the offence would involve either dispensing with the first part of the public element of the offence or substantially extending its meaning and would therefore amount, impermissibly, to judicially extending the boundaries of criminal liability.[149]

6.136 Even if the domestic common law offence was interpreted narrowly in this way, it is clear that there are multiple other criminal charges that could apply to online communications which “outrage” public decency (such as the communications offences under section 127 of the CA 2003).

6.137 However, should the courts in England and Wales decide that the Internet *is* a public place, a further question for the offence of outraging public decency would be whether the same offline “minimum standards of decency” apply to the online world. While an act itself may outrage public decency in the offline world, would it do so similarly in the online world, where the standard of images and videos available may on the whole be more indecent than what one would find in the “real world”? This question cannot yet be answered, but it demonstrates the complex challenges that may arise when applying this common law offence to online communication.

“EXPOSURE” UNDER SECTION 66 OF THE SEXUAL OFFENCES ACT 2003

6.138 A person commits an offence of exposure under section 66 of the Sexual Offences Act 2003 if:

(a) he intentionally exposes his genitals, and

(b) he intends that someone will see them and be caused alarm or distress.[150]

6.139 The offence is an “either-way offence”. On summary conviction, a person is liable for a maximum sentence of six months’ imprisonment or a fine. On indictment, a person is liable for a maximum sentence of two years’ imprisonment.[151]

6.140 The offence is one of specific intent, and voluntary intoxication from alcohol or drugs, may be a defence if it meant the defendant did not form the requisite intent because of intoxication.[152]

6.141 Exposing genitals solely for the purpose of sexual gratification would not be sufficient to satisfy the commission of the offence.

---

149 *HKSAR v Chan Yau Hei* [2014] HKCFA 18; (2014) 17 HKCFAR 110 at [50].

150 Sexual Offences Act 2003, s 66(1).

151 Sexual Offences Act 2003, s 66(2).

152 M Stevenson, *Indecent Exposure* (11 September 2018) available at https://login.westlaw.co.uk/maf/wluk/app/document?&srguid=i0ad69f8e00000166a5a5966ac464a0ba&docguid=I591E72F073DA11E4981F97CD1F3E26F4&hitguid=I591E72F073DA11E4981F97CD1F3E26F4&rank=1&spos=1&epos=1&td=1&crumb-action=append&context=33&resolvein=true.

6.142 The Act does not prescribe where the offence can occur. As such, exposure may be committed in a public or private space.[153]

6.143 The courts have accepted the application of the offence of exposure to online communication. In *R v Alderton*,[154] for example, the defendant was charged (along with a number of other counts involving engaging in sexual activity with a child) with six counts of exposure under section 66, for exposing his genitals while on Facetime with the victim.

6.144 Given that exposure relates to an act in real-time rather than the distribution and possession of images or recordings, the online application of the offence of exposure may only apply to "live streamed" online communication, such as Facetime or Skype, as opposed to communication which require recording and subsequent sending of a video, such as Snapchat. However, this is yet to be confirmed in law.

POSSESSION OF AN EXTREME PORNOGRAPHIC IMAGE UNDER THE CRIMINAL JUSTICE AND IMMIGRATION ACT 2008

Introduction

6.145 While the OPA 1959 offences target the production and distribution of obscene material, the Criminal Justice and Immigration Act 2008 ("CJIA 2008") creates an offence for "a person to be in possession of an extreme pornographic image".[155]

6.146 This legislation was enacted after the conviction of Graham Coutts in 2005[156] for the murder of Jane Longhurst. When arrested for the murder, he was found to be in possession of a significant amount of violent pornographic images. His rate of downloading those images declined in the weeks after the murder.[157] This sparked a widespread campaign to criminalise possession of these types of images, based on the perception that possession of extreme pornography could lead to seriously deviant behaviour in the "real world".[158] Some academics, such as Hornle, have criticised this rationale, noting that there is little evidence that suggests possessing extreme pornography results in actual harm.[159] In 2014, however, it was suggested in the House of Lords that, although there may not be a substantial link between the possession of extreme pornographic images and the perpetration of sexual violence, the distribution

---

153 M Stevenson, *Indecent Exposure* (11 September 2018) available at https://login.westlaw.co.uk/maf/wluk/app/document?&srguid=i0ad69f8e00000166a5a5966ac464a0ba&docguid=I591E72F073DA11E4981F97CD1F3E26F4&hitguid=I591E72F073DA11E4981F97CD1F3E26F4&rank=1&spos=1&epos=1&td=1&crumb-action=append&context=33&resolvein=true.

154 [2014] EWCA Crim 2204.

155 Criminal Justice and Immigration Act 2008, s 63(1).

156 *R v Coutts* [2006] UKHL 39; [2005] 1 WLR 1605.

157 *R v Coutts* [2006] UKHL 39; [2005] 1 WLR 1605. Also discussed in A Murray, "The Reclassification of Extreme Pornographic Images" (2008) *Modern Law Review* 73.

158 See, eg Home Office and Scottish Executive, *Consultation: On the possession of extreme pornographic material* (August 2005), available at http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/30_08_05_porn_doc.pdf.

159 See, eg J Hornle, "Countering the dangers of online pornography – Shrewd regulation of lewd content" (2011) 2(1) *European Journal of Law and Technology* 9.

and possession of such material has the potential to create a climate in which people are more exposed to sexual violence and whereby such behaviour may not be taken as seriously as it should.[160]

6.147 The move to criminalise possession, in addition to publication, sought to address jurisdictional barriers to prosecution under the OPA 1959, and to provide an offence enforceable when material is sourced and distributed from abroad.[161]

The offence

6.148 For the section 63(1) of the CJIA 2008 offence to be committed, the image must be "pornographic" and "extreme".

6.149 An image means a "moving or still" image produced by any means, or "data (stored by any means) which is capable of conversion into an image".[162]

6.150 Under section 63(7) and (7A) CJIA 2008, the image must portray the prescribed acts in an "explicit and realistic way" to be considered extremely pornographic. Some cartoons, illustrations or other such drawings might not be captured under this legislation.

6.151 The content of the material itself, rather than the state of mind of the reader, is considered for the purposes of the CJIA 2008. We explore this further below.

6.152 The offence is triable either way. On summary conviction, it is punishable with a maximum penalty of 6 months' imprisonment or fine, or both. On indictment, the maximum penalty that may be imposed is three years' imprisonment for images portraying acts that are life threatening or inflict serious injury, or involve portrayals of non-consensual penetration, and two years' imprisonment for acts of bestiality or necrophilia. Both cases may also attract an unlimited fine.[163]

6.153 Proceedings under section 63 of the CJIA 2008 may not commence without consent of the Director of Public Prosecutions,[164] to safeguard against possible overcriminalisation including unnecessary prosecutions that are not in the public interest.[165]

Meaning of "pornographic"

6.154 Section 63(3) of the CJIA 2008 defines an image as pornographic if it can "reasonably be assumed to have been produced solely or principally for the purpose of sexual

---

160 Legislative Scrutiny: (1) Criminal Justice and Courts Bill, Joint Committee on Human Rights (2013-14) HL 189, HC 1293, paras 1.42 and 1.43.

161 See, eg Home Office and Scottish Executive, *Consultation: On the possession of extreme pornographic material* (August 2005), available athttp://news.bbc.co.uk/1/shared/bsp/hi/pdfs/30_08_05_porn_doc.pdf; see also J Rowbottom, "Obscenity laws and the internet: targeting the supply and demand" [2006] *Criminal Law Review* 97; and J Hörnle, "Countering the dangers of online pornography – Shrewd regulation of lewd content" (2011) 2(1) *European Journal of Law and Technology* 9.

162 Criminal Justice and Immigration Act 2008, s 63(8).

163 Criminal Justice and Immigration Act 2008, s 67.

164 Criminal Justice and Immigration Act 2008, s 63(10).

165 Crown Prosecution Service, "Extreme Pornography", available at https://www.cps.gov.uk/legal-guidance/extreme-pornography.

arousal". Simply having a sexual dimension is not automatically sufficient for the image to be pornographic; sexual arousal must be the sole or principal purpose.[166]

6.155 However, the purpose of the initial producer (such as the initial photographer of an image), and the circumstances of how the image is eventually received, have been said to be "irrelevant"[167] and "immaterial".[168]

6.156 In the case of *R v Baddiel*,[169] the accused had received images in a series of WhatsApp messages that were subsequently found on his phone and computer (where, under the application's default setting, they are automatically stored when messages are opened in WhatsApp). On appeal, the appellant argued that the "purpose" for section 63(3) must be that of the sender in the WhatsApp group, which was argued to be humorous, rather than the initial photographer, whose purpose may well have been for sexual arousal.

6.157 The Court of Appeal rejected this submission, stating that section 63(3):

> means simply was it produced (and by whom is utterly immaterial) for the purpose of sexual arousal of anyone who comes to have it, be that the producer himself, a distributor or ultimate recipient.[170]

6.158 This approach potentially extends criminal liability under section 63 to a wide range of people who are the recipients of images sent online. Anyone who has received an extreme pornographic image may be committing the offence if that image is retained on their online platform, such as in their Facebook private message inbox or WhatsApp inbox. This could be the case regardless of the spirit in which the image was sent, and whether or not the recipients asked for the image or intended for it to be kept on their devices.

6.159 Section 63(4) of the CJIA 2008 provides that if an image is found in a series of other images, the question whether the image is pornographic is "determined by reference to the image itself; and (if the series of images is such as to be capable of providing a context for the image) the context in which it occurs in the series of images".

6.160 Section 63(5) of the CJIA provides the following clarification:

> So, for example, where –
>
> (a) an image forms an integral part of a narrative constituted by a series of images; and

---

166 Ministry of Justice, *Possession of Extreme Pornographic Images and increase in the maximum sentence for offences under the Obscene Publications Act 1959: Implementations of sections 63-67 and Section 71 of the Criminal Justice and Immigration Act 2008* (19 January 2009), p 3, available at http://webarchive.nationalarchives.gov.uk/20110204180014/http://www.justice.gov.uk/publications/docs/circular-criminal-justice-01-2009(1).pdf.

167 *R v Baddiel* [2016] EWCA Crim 474; [2016] 1 WLR 4157 at [16].

168 *R v Baddiel* [2016] EWCA Crim 474; [2016] 1 WLR 4157 at [15].

169 [2016] EWCA Crim 474; [2016] 1 WLR 4157.

170 *R v Baddiel* [2016] EWCA Crim 474; [2016] 1 WLR 4157 at [15].

(b) having regard to those images as a whole, they are not of such a nature that they must reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal,

the image may, by virtue of being part of that narrative, to be found not to be pornographic, even though it might have been found to be pornographic if taken by itself.

6.161 This seems designed to apply to, for example, scenes in a movie. However, it is less easily applied in relation to certain sorts of online communication: for example, whether a number of images in files on the Cloud, WhatsApp messages, or a line of private messages on Facebook would constitute part of a series. In this type of case, the court would have to consider matters such as the time between sending each message, or, if the messages were each sent by different people (for example numerous members in a WhatsApp group), to determine whether an image constituted part of a series.

Meaning of "extreme"

6.162 For an image to be "extreme" it must depict (explicitly and realistically) any of a discrete number of acts listed in subsections (7) or (7A) and be of "grossly offensive, disgusting or otherwise of an obscene character".[171]

6.163 The words "grossly offensive" and "disgusting" are not alternatives to "obscene character" but are examples of it. Drawn from the ordinary dictionary definition of "obscene", they reflect different aspects of that concept, and are intended to convey a non-technical understanding of it. The term is distinct from the technical definition contained in the OPA 1959, which is specifically geared to the concept of publication.[172]

6.164 Section 63(7) of the CJIA 2008 includes images portraying, in an explicit and realistic way:

(a) an act which threatens a person's life;

(b) an act which results, or is likely to result, in serious injury to a person's anus, breast or genitals;

(c) an act which involves sexual interference with a human corpse; or

(d) a person performing an act of intercourse or oral sex with an animal (whether dead or alive).

6.165 Section 63(7A) of the CJIA 2008 includes images portraying explicitly and realistically "an act which involves the non-consensual penetration of a person's vagina, anus or mouth by another with the other person's penis" or "an act which involves the non-

---

171 Criminal Justice and Immigration Act 2008, s 63(5A).

172 Ministry of Justice, *Possession of Extreme Pornographic Images and increase in the maximum sentence for offences under the Obscene Publications Act 1959: Implementations of sections 63-67 and Section 71 of the Criminal Justice and Immigration Act 2008* (19 January 2009), p 3, available at http://webarchive.nationalarchives.gov.uk/20110204180014/http://www.justice.gov.uk/publications/docs/circular-criminal-justice-01-2009(1).pdf.

consensual penetration of a person's vagina or anus by another with a part of the other person's body or anything else".[173]

6.166 The image will only fall within either subsection if a reasonable person looking at the image would think that the people or animals in it were real.

6.167 Both subsections 63(7) and (7A) CJIA 2008 include reconstructed genitalia, for example by way of gender reassignment.[174]

6.168 The CPS guidance[175] states that while all "extreme" material can be considered obscene, "not all obscene material is extreme". Thus, these provisions would appear to cover a more limited range of material than that covered by the OPA 1959 and section 127 of the CA 2003.[176] However, some overlap between these different offences is inevitable. We explore this further below.

Images portraying acts which result, or are likely to result, in "serious injury"

6.169 The Ministry of Justice notes that portrayal of acts inflicting "serious injury" could include portrayal of "hanging, suffocation or sexual assault with the threat of a weapon".[177]

6.170 The CPS guidance also advises prosecutors that it will often not be in the public interest to prosecute for images portraying acts causing serious injury unless there are aggravating factors present. These include the extent of circulation, evidence of exploitation, number of images and prior conduct.[178]

6.171 The CPS guidance also notes the need to have regard to the right to a private life and that the interference with this right must be "proportionate and necessary".[179]

6.172 The specificity of the body parts listed in section 63 as at risk of being harmed or likely to be harmed has been criticised. McGlynn and Rackley, for example, note the potential

---

173 This was inserted by section 37 of the Criminal Justice and Courts Act 2015 and does not apply to possession of an image prior to 13 April 2015.

174 Criminal Justice and Immigration Act 2008, s 63(9).

175 Crown Prosecution Service, *Extreme Pornography*, available at https://www.cps.gov.uk/legal-guidance/extreme-pornography.

176 Crown Prosecution Service, *Extreme Pornography*, available at https://www.cps.gov.uk/legal-guidance/extreme-pornography.

177 Ministry of Justice, *Possession of Extreme Pornographic Images and increase in the maximum sentence for offences under the Obscene Publications Act 1959: Implementations of sections 63-67 and Section 71 of the Criminal Justice and Immigration Act 2008* (19 January 2009), p 2, available at http://webarchive.nationalarchives.gov.uk/20110204180014/http://www.justice.gov.uk/publications/docs/circular-criminal-justice-01-2009(1).pdf.

178 Crown Prosecution Service, *Extreme Pornography*, available at https://www.cps.gov.uk/legal-guidance/extreme-pornography.

179 The guidance was revised after the case of *R v Walsh (Simon)* (8 August 2012) Crown Court - Kingston (unreported); see E Rackley and C McGlynn, "Prosecuting the possession of extreme pornography: a misunderstood and mis-used law" [2013] *Criminal Law Review*, 400.

for "ludicrous results with some injuries being proscribed, others not".[180] Further, they state that this has been said to disregard the harm and impact imposed by extreme pornography as a whole, "at least partly, a result of the Government's failure to set out and address directly the nature of the harm in extreme pornography".[181]

Meaning of "possession" and defences under section 65(2) of the CJIA 2008

6.173 Section 65(2) of the CJIA 2008 provides for the following defences:

(a) that the person had a legitimate reason for being in possession of the image concerned;

(b) that the person had not seen the image concerned and did not know, nor had any cause to suspect, it to be an extreme pornographic image;

(c) that the person –

(i) was sent the image concerned without any prior request having been made by or on behalf of the person, and

(ii) did not keep it for an unreasonable time.

6.174 These defences come down to the nature and definition of "possession".

6.175 This can be a challenging concept to apply in an online world where "storing" of files can occur automatically and temporarily as part of the technical operation of a device (for example, the random access memory of a computer, where stored data could be lost if power is removed), and also stored but not necessarily opened by a user.

Meaning of "possession"

6.176 The case of *R v Cheung*[182] highlighted that there are two elements of possession that must be satisfied for the purposes of the section 66 offence; physical possession and mental possession. Drawing on the judgments in cases of possession of drugs such as *Warner v Metropolitan Police Commissioner*,[183] *R v McNamara*,[184] *R v Brooks*,[185] and *R v Lambert,*[186] the Court of Appeal in *Cheung* reiterated that possession requires both physical and fault elements, as it does for the purposes of the Misuse of Drugs Act 1971.

---

180 C McGlynn and E Rackley, "Criminalising extreme pornography: a lost opportunity" [2009] 4 *Criminal Law Review* 245, p 248.

181 C McGlynn and E Rackley, "Criminalising extreme pornography: a lost opportunity" [2009] 4 *Criminal Law Review* 245, p 248.

182 [2009] EWCA Crim 2965.

183 [1962] 2 AC 256.

184 (1988) 87 Cr App R 246.

185 [1974] AC 862.

186 [2002] QB 1112.

6.177 For physical possession to be satisfied, the prosecution must prove that the defendant had "custody and control" of the image. This is a question of fact for the jury. In line with the approach outlined in *Lambert*,[187] unless the thing is in the control of the defendant, it cannot be in his or her possession, even if it is in their custody.

6.178 In addition, the prosecution must prove mental possession: that the defendant had knowledge of the images in question (but not knowledge of the requisite quality of the images, explained further below). Usually, mental possession will follow from physical possession (for example, the defendant was in custody and control of a transparent container, they would likely know what was in the container). However, in some cases there may be physical possession without mental possession (the container is not transparent, and although the defendant has control and custody of the container, someone put something in there without them knowing).[188]

6.179 In the case of *Cheung*,[189] the defendant was found in possession of a number of DVDs in a bag given to him by a friend, some of which contained extreme pornographic images. The defence argued that while the defendant knew he was carrying DVDs, he had no knowledge that some showed extreme pornography, and there was no forensic evidence to suggest he had handled those that did.

6.180 The Court of Appeal held that in order to show possession, the prosecution only had to prove the defendant knew that the bag he was carrying had DVDs in it, and not that he knew the DVDs were extremely pornographic (unless there was a doubt as to whether the defendant believed, for example, that the "things" in his possession were not DVDs at all but something wholly different).

6.181 The defendant's awareness that he or she possesses articles will be an important question when the facts of a case involve online communication. For example, although a private message in a defendant's Facebook private message inbox is in their custody and control, they may not have checked their inbox, or opened the message, to know that it contained extremely pornographic images. In these circumstances, it is likely that mental possession would not be satisfied.

6.182 A similar question was raised in the case of *Baddiel*,[190] described at paragraph 6.156. The defendant was convicted of possession of the images on his iPhone but not on his computer. Images were stored on his computer automatically when he deleted them from his phone. However, records showed that he had deleted the images from his phone weeks after receiving them via WhatsApp. The jury decided that the delay meant that the storing of images on his phone, regardless of ultimate deletion, did constitute possession.

---

187 *R v Lambert* [2002] QB 1112.

188 D Selfe, "Case comment: Extreme pornographic images – mens rea and defences" (2011) 200 *Criminal Lawyer* p 4.

189 *R v Cheung* [2009] EWCA Crim 2965.

190 *R v Baddiel* [2016] EWCA Crim 474; [2016] 1 WLR 4157.

Defendant had not seen the image

6.183 In cases where a defendant intends to rely on section 65(2)(b), once physical possession is established, the onus then switches to the defendant to prove on the balance of probabilities that they had not seen the image concerned and did know nor have any cause to suspect it to be an extreme pornographic image.[191]

6.184 The section below on "online considerations" will consider the implications the judgment of *R v Cheung*[192] might have for the online world. Knowing, for example, you have a file on your computer, phone or Dropbox – even if shared with another person – may be sufficient to satisfy the possession requirement. It will then be up to a defendant to make out a defence under section 65(2).

Deleted images

6.185 When viewing internet images on a computer screen, the hard drive keeps a record of those images, stored in what is known as a "cache". Following the decision in *Atkins v DPP*[193] (although in relation to possession of indecent images of a child), anything stored in a cache will be considered to be in a person's possession. As such, so long as there was proof of knowledge of the cache, the person could be convicted for possessing extreme pornography.

6.186 In the case of *R v Porter*,[194] the Court of Appeal considered the notion of possession in relation to indecent photographs of children, specifically the images that had been deleted and were in the applicant's recycle bin folder. Although the case related to possession in section 160(1) of the Criminal Justice Act 1988, the discussion is of interest for these purposes. The Court held that, where images have been deleted, it is for the jury to decide whether a defendant has custody or control of the image taking into account their knowledge, including whether they could retrieve or access the image.[195]

6.187 This way of understanding "possession", however, has been of some concern. While knowledge of how to recover a deleted image may suggest that image is still in a person's possession, Akdeniz has argued that cases like *Porter*[196] have imposed a subjective element to a physical concept.[197] He argued that it implies that only the

---

191 *R v Cheung* [2009] EWCA Crim 2965 at [16]; discussed also in D Ormerod and D Perry (eds), ***Blackstone's** Criminal Practice 2019*, para B3.349.

192 [2009] EWCA Crim 2965.

193 [2000] 1 WLR 1427.

194 [2006] EWCA Crim 560; [2006] 1 WLR 2633.

195 Discussed also in C McGlynn and E Rackley, "Criminalising extreme pornography: a lost opportunity" [2009] 4 *Criminal Law Review* 251.

196 *R v Porter* [2006] EWCA Crim 560; [2006] 1 WLR 2633.

197 Y Akdeniz, "Possession and Dispossession: a critical assessment of defences in possession of indecent photographs of children cases" [2007] *Criminal Law Review* 274, p 283.

computer illiterate would be able to rely on this defence, and it may not be available to those who know how to recover deleted images.[198]

Defence for participants in images where no non-consensual harm on another

6.188 Section 66 of the CJIA 2008 provides a further defence for possession of extreme pornographic images – except those involving necrophilia (with a real corpse)[199] or bestiality – if the accused person is a direct participant in the acts portrayed by the images, and the act did not actually involve inflicting non-consensual harm on another.[200]

6.189 The Act defines non-consensual harm as:

(a) the harm is of such a nature that the person cannot, in law, consent to it being inflicted on himself or herself; or

(b) where the person can, in law, consent to it being so inflicted, the person does not in fact consent to it being so inflicted.[201]

ONLINE CONSIDERATIONS

6.190 This section uses fictional examples to illustrate some of the challenges in prosecuting communications offences relating to obscenity and indecency when the offending behaviour happens online. These challenges include:

(a) ease of commission of the offences;

(b) the vagueness and breadth of the offences when applied to online communication, including the dangers of overcriminalisation and ensuring adequate protection of the right to freedom of expression; and

(c) jurisdictional issues.

---

198 See also D Ormerod, "Indecent Photograph of a Child" [2006] *Criminal Law Review* 748, p 751.

199 In the case of necrophilia, in order to rely on the defence at section 66 the accused must prove that the act did not involve a real corpse.

200 See D Ormerod and D Perry, *Blackstone's Criminal Practice 2019*, para B3.349; Ministry of Justice, "*Further information on the new offence of Possessing Extreme Pornographic Images and increase in the maximum sentence for offences under the Obscene Publications Act 1959: Implementations of sections 63-67 and Section 71 of the Criminal Justice and Immigration Act 2008* (19 January 2009), p 5, available at http://webarchive.nationalarchives.gov.uk/20110204180014/http://www.justice.gov.uk/publications/docs/circular-criminal-justice-01-2009(1).pdf.

201 Criminal Justice and Immigration Act 2008, ss (3)(a) and (b). Note, however, that this relates to the level of harm that cannot be consented to, and not whether or not a person has consented. The latter is dealt with elsewhere; for example, Sexual Offences Act 2003, s 74. For further discussion on consent, see M Lucraft, *Archbold Criminal Pleading Evidence and Practice 2019* (2018), Chapter 20: Sexual Offences, paras 20-29 to 20-32.

Ease of commission

Example 1:

Grant, a sixteen-year-old boy, sends a video including images of necrophilia to a number of his contacts via Snapchat.

Glen opens the Snapchat and takes a screenshot of the video.

Grace opens the Snapchat and views it for 10 seconds until it goes away.

Amanda can see that she has a Snapchat from Grant but does not open the Snapchat. She leaves it on her phone unopened.

Analysis

6.191 The main offences that need to be considered here are: the obscene publication offence under the OPA 1959 and obscene or indecent communication under section 127 of the CA 2003 (for Grant) and the possession of extreme pornography offence as per section 63 of the CJIA 2008 (for Glen, Grace and Amanda).

6.192 Grant could be prosecuted under section 2 of the OPA 1959. The type of behaviour depicted in the video could be considered "obscene" as it would tend to "deprave and corrupt" the likely audience (in this case, those who received his Snapchat). By sending the video via Snapchat, Grant is transmitting data and therefore "publishing" it according to the definition under section 2(3)(b) of the OPA 1959.

6.193 In addition, the video is part of a message of that is of an indecent nature sent by means of a public electronic communications network and would fall within section 127 of the CA 2003.

6.194 The video is also extremely pornographic under section 63(7)(d) of the CJIA 2008. As a result, Glen, Grace, and Amanda may be committing an offence of possessing extreme pornography. Whether each has in fact committed the offence will be likely to rest on whether they each "possess" the video for the purposes of section 63 of the CJIA 2008.

6.195 If Glen retains the screenshot of the video, it is likely that he will be possessing it for purposes of section 63 and could be prosecuted (subject to a prosecution being in the public interest under the CPS Code).

6.196 It is unlikely that Grace would satisfy the element of possession, because although she viewed the video she is unable to retrieve it once the 10 seconds expires after opening. The image is not stored on her device thereafter. Even if viewing of the video was considered to be possession, she did not keep it for an unreasonable time and would potentially have a defence under section 65(2) of the CJIA 2008.

6.197 Although she has not viewed the video, Amanda would be likely to satisfy the possession element of section 63 because it remains stored on her phone. Following

the approach in *R v Cheung*,[202] even if she did not know what the image contained, she knew she had an image from Grant and that would be sufficient for "possession". The burden would then fall on her to establish a defence under section 65(2)(b). This should be successful: she did not see the image in her possession (as it was unopened) and she had no reason to suspect it was extremely pornographic (Snapchat does not preview images that are received; there is no way to tell what the Snapchat contains unless it is opened).

6.198 This example demonstrates the way in which unsolicited receipt of certain types of messages may make a person liable under section 63 of the CJIA 2008 offence. It also illustrates the potential breadth of application of these offences. It is clear that the offences overlap in the same set of factual circumstances in particular in an online context. However, liability online can also depend on the platform chosen by the sender, which may not be an appropriate way to determine criminal responsibility for a crime of possession.

Example 2:

In a private encrypted group on the instant messaging service Telegram, a group of men are discussing their violent sexual fantasies. One of the men, Steve, doesn't send any messages to the group itself; he simply enjoys reading what the others in the group send.

Analysis

6.199 In this example, the possible offences being committed are an obscene publication under the OPA 1959 and obscene or indecent communication under section 127 of the CA 2003.

6.200 Steve could not be prosecuted for an offence under the OPA 1959. He has not published anything – understood in this case as the transmission of data – for the purposes of the Act.

6.201 Steve also has not "sent" any messages and could not be prosecuted under section 127 of the CA 2003. However, it could be argued under section 127(1)(b) of the CA 2003 that Steve caused a message to be sent, by being a part of the group.

6.202 The others in the group who did send messages may be guilty of offences under section 2 of the OPA 1959 or section 127 of the CA 2003.

6.203 The messages, although only in text format, may constitute obscene "articles" following the *Smith* case. As data has been transmitted, the messages are likely to be "publications". The messages are also likely to be considered indecent. As such, the senders may also be committing an offence under section 127 of the CA 2003.

6.204 Further consideration may need to be given to the different formats of communication online (the differences, for example, between sending obscene or indecent messages

[202] [2009] EWCA Crim 2965.

via a private and encrypted messaging service and a similar message in a public post). Different forms of online communication may fall at different points in the spectrum from private to public. If the purpose of the communications offences is to protect the "propriety" of a *public* electronic communications network, it is not clear that the offences ought to apply to private online communication within an essentially private setting (for example, an encrypted messaging service). This example demonstrates the potential overcriminalisation of obscenity and indecency online and highlights the need for further consideration in balancing the intentions behind these offences with the need to protect the right to freedom of expression.

Vagueness and malleability of "indecency" and "obscenity"

> **Example 3:**
>
> Angela and Mark record themselves naked and taking cocaine and consensually post it on their own Twitter page. They mark it as sensitive material.
>
> Their friend, Tim, re-tweets their video. He also marks it as sensitive material.

Analysis

6.205 There are a number of offences that may apply to the video posted and reposted in these circumstances: section 2 of the OPA 1959, section 127 of the CA 2003, the IDPA 1981 and the common law offence of outraging public decency.

6.206 In order for the OPA 1959 offence to apply, the video must be "published", and obscene.

6.207 As the posting required a transmission of data, there is a publication.

6.208 The Court in *John Calder (Publications) Ltd v Powell*[203] concluded it was possible for "obscenity" to extend beyond sexual imagery, to depictions of drug taking. Using this approach, it is possible that Angela and Mark's video may be considered "obscene", so long as it tends to deprave or corrupt a significant portion of the likely audience.

6.209 Marking the content sensitive will limit the likely audience to those who would opt in to see sensitive content.

6.210 Any Twitter user – that is, people as young as thirteen years old – can opt in to see media that may contain sensitive content.[204] As such, merely marking an image or video as "sensitive" does not stop young people from potentially viewing the content.

6.211 If children are likely to see Angela and Mark's video (and make up a not insignificant proportion of the audience) then the article should be assessed by this standard. This may mean that the video posted on Twitter would constitute an obscene publication, on

---

[203] [1965] 1 QB 509.

[204] See, eg Twitter, *Report sensitive media*, available at https://help.twitter.com/en/safety-and-security/sensitive-media.

the basis that children as young as thirteen – who are allowed, under Twitter internal policies, to use the platform – could be likely readers.

6.212 However, even if it can be argued that the likely audience of Twitter users (which includes children thirteen years old and over) are already corrupted (by way of having already viewed sensitive material of a similar nature), the video may still tend to (further) deprave or corrupt.[205]

6.213 The sensitivity notice that may be applied by uploaders would not be sufficient, considering that child users may still view the material. It is therefore possible that Angela and Mark have committed an offence under section 2 of the OPA 1959.

6.214 On similar reasoning, Tim could also be charged under the OPA 1959 for re-tweeting the video.

6.215 Although there is no definition or guidance on what may be considered "indecent", this video could also be considered "indecent" as it is likely that most right-minded people would consider drug-taking to be an indecent act (and the recording of such an indecent communication). However, it is unclear at what point this would cross the threshold from "indecent" to "obscene" (if they are considered to be at opposite ends of the scale). Nevertheless, a prosecution may be brought under section 127 of the CA 2003 which includes communication of an indecent *or* obscene nature.[206] Posting it on Twitter would constitute transmission of data which means that Angela, Mark and Tim could all be committing an offence under section 127 of the CA 2003.

6.216 Other possible offences include the offence of indecent display under the IDCA 1981 and the common law offence of outraging public decency.

6.217 The video may be considered indecent for the purposes of the IDCA 1981. However, the question then arises as to whether the social media platform could be considered a "public place". Under section 1(3) of the IDCA 1981 a public place is "any place to which the public have or are permitted to have access (whether on payment or otherwise) while that matter is displayed".

6.218 However, the law is not yet clear on how this would apply to the online world. One possibility is that, using the definition in section 1(3) of the IDCA 1981, Angela and Mark's Twitter page – and their drug video displayed on that page – may be considered a public place because all people (provided they are thirteen or over) have access to it. Marking the video as sensitive material on Twitter would not be a sufficient warning under section 1(3) of the IDCA 1981, for the reasons stated at paragraph 6.210 above.

6.219 If their video had been posted on some other platform which allowed it to be hidden behind a paywall, particularly with age verification, they may not be committing an offence under IDCA 1981.

---

205 *DPP v Whyte* [1972] AC 849.

206 It also includes communication of a grossly offensive nature, discussed in Chapter 5.

6.220 However, if we rely on the approach taken in *HKSAR v Chan Yau Hei*,[207] Twitter or any other online platform would not be a public place for the purposes of the IDCA 1981.

6.221 Re-tweeting could also be considered a display for the purposes of the IDCA, and Tim may also be liable to prosecution for an offence under IDCA 1981.

6.222 For the purposes of outraging public decency, there are two questions to answer: whether the video outrages public decency and whether the Twitter page is a public place for the purpose of the common law offence (that is, if it passes the "two-person rule").

6.223 In relation to the first question, it is likely that the minimum standards of decency require people not to be exposed to videos of drug taking (particularly when people as young as thirteen may be exposed to such content). Given that anyone, including children as young as thirteen, can opt in to viewing sensitive content, it could be argued that even content marked sensitive should adhere to some element of decency. However, it is unclear in law whether that is the case. A publicly available video of drug taking may therefore outrage the minimum standards of decency, but the law is still yet to apply the offence to online communication.

6.224 The second question, however, is more complex. The Twitter page would pass the "two-person test" and could be considered "public" in the sense that posts on Twitter are widely available and accessible to much more than two people. However, the approach in *Chan Yau Hei*[208] if adopted, also means that for the purposes of outraging public decency, Twitter cannot be considered a public place.

6.225 It remains to be seen whether such online platforms are considered public places in this jurisdiction.

6.226 This example also shows the potential breadth of these offences and their overlap in relation to online communication. While section 127 of the CA 2003 may be the only possible offence to apply to the circumstances in the example above, it suggests a need to answer the question whether or not the online environment – or particular means of online communication – can be considered a public place.

6.227 Further, clarity in law could help unwitting potential offenders, police and prosecutors to discern which threshold may apply to this type of conduct, and what is the most appropriate criminal offence to reflect the harm caused.

---

207 [2014] HKCFA 18; (2014) 17 HKCFAR 110.

208 *HKSAR v Chan Yau Hei* [2014] HKCFA 18; (2014) 17 HKCFAR 110.

Jurisdictional issues

Example 4:

Graham is on holiday in the United States. He uses a BitTorrent client to download an obscene movie.

A BitTorrent client is a desktop application that initiates, truncates and manages the downloading and uploading of data (usually for videos such as movies and television shows, or music). The BitTorrent allows a user to download a movie (for example) by gathering pieces of the file and downloading these pieces simultaneously from people who already have them.

The BitTorrent client is still on when Graham turns on the laptop and starts using it.

Once on, BitTorrent client will use the pieces of the file that he has on his laptop (in this case, the obscene movie) along with pieces of the same file from other uses, for people who want to download the same video. The transmitting of these file pieces is called "seeding" and, once put together, results in someone "downloading" the video.

Graham doesn't realise this is how BitTorrent works. As a result, by having his laptop on while on holiday in the United States, he is unwittingly allowing other BitTorrent users to seed and download the video. Some BitTorrent users in England have downloaded the obscene movie.

Analysis

6.228 This example also demonstrates the complex multi-jurisdictional nature of the online environment, and the challenges that may arise when people based in different countries make content available in England and Wales, which may be illegal in this jurisdiction, but legal and protected in the country in which they are acting.

6.229 In this case, Graham may have committed an offence under the OPA 1959 or section 127 of the CA 2003.

6.230 First, it is clear that there has been a transmission of data and therefore publication. However, Graham's BitTorrent seeding of the obscene movie is being done from his laptop in the United States. This is a different jurisdiction to where the data is being downloaded; for example, the BitTorrent users in England who have downloaded the obscene movie.

6.231 While Graham did not actively send or transmit data to others in England, based on the approach in *R v Waddon,*[209] relied on in *R v Perrin*,[210] the mere fact he has made the obscene material "available" in England means that he has committed an obscene

[209] [2000] All ER (D) 502.

[210] [2002] EWCA Crim 747.

publication offence in England (under either section 2 of the OPA or section 127 of the CA 2003).

6.232 Graham could use the substantial measure test to argue that the crime was committed in the United States. Graham would need to argue that a substantial measure of the crime did not occur in England and Wales. In this case, he could prove that the data was "published" or "sent" (depending on whether he is being prosecuted under section 2 of the OPA 1959 or section 127 of the CA 2003) – by way of seeding – while he was in the United States. However, Graham could be prosecuted on the basis of the terminatory theory, regardless of where the initial transmission of data actually took place. This is because the citizens of England are being affected by the conduct (they are being depraved and corrupted by way of having an obscene movie available to be downloaded by them).

6.233 This example suggests that if every country adopted the approach in *R v Perrin*[211] and *R v Waddon*, [212] then a person could find themselves committing criminal offences in multiple countries, even in circumstances where what they were doing was lawful in the country from which they were acting. To ensure they avoid criminal liability, there is a risk that people will have to comply with the strictest safeguards in the world, which may have the effect of chilling free speech.

CONCLUSION

6.234 This Chapter has identified a number of challenges with applying obscenity and indecency offences to the online world:

(1) the vagueness and malleability of the concepts underlying these offences, including what is "obscene" or "indecent";

(2) the fact that their application of what is "obscene" or "indecent" may overlap in online communications;

(3) the potential for the OPA 1959 to criminalise private online conversations;

(4) whether the online environment, or specific online platforms, are "public places" for the purposes of outraging public decency and the IDCA 1981;

(5) the problematic interpretation of "possession" in relation to the CJIA 2008 for online platforms; and

(6) enforcement and prosecution challenges when material is "published" in another jurisdiction.

6.235 Many of the offences described in this Chapter were introduced long before cyberspace changed the way we "publish", "transmit", "possess" information and conceptualise public space.

---

211 [2002] EWCA Crim 747.

212 [2000] All ER (D) 502.

6.236 In some cases, the current law may criminalise online communication in ways that would not apply to offline communication, potentially interfering with the right to freedom of expression.

6.237 The elements of these offences need to be carefully considered in the context of the online world, to ensure the law is as effectively governing online communication as it would offline communication, and achieving the right balance between protecting people from abusive and offensive content and protecting their right to freedom of expression.

Chapter 7: Threatening communications

INTRODUCTION

What is a threat in criminal law?

7.1 In its ordinary meaning, a threat is a statement of intention to cause a harmful consequence.

7.2 In the criminal law of England and Wales, however, there is no general offence of threatening either to commit a crime or to cause harm, no legal definition of a threat[1] and no coherent structure of threat offences. Instead, there is a patchwork of different statutes which criminalise specific types of threat.[2]

7.3 In this Chapter, we set out the protection the criminal law provides to the victims of threats, and analyse whether victims of threats made online are afforded the same protection under the law as victims of threats made offline.

Offences including requirement of threat

7.4 There are a number of statutory offences of making threats.

7.5 A threat to kill is an offence contrary to section 16 of the Offences Against the Person Act 1861 ("OAPA 1861").

7.6 A threat of immediate violence to an individual might also be punishable:

(1) as a common assault or;

(2) under various provisions in the Public Order Act 1986 ("POA 1986").

---

1 Whether or not behaviour is threatening is a matter of fact to be left to the jury or magistrates' court.

2 Examples of statutes containing threat offences which we do not consider in the context of this Report on abusive and offensive online communications include (1) those where the offence is primarily one of acquisition rather than abuse see, eg Theft Act 1968, s 21 (blackmail); Unsolicited Goods and Services Act 1971, s 2(2)(b) (demanding payment for unsolicited goods); Public Order Act 1986, s 38 (contamination or interference with goods with the intention of causing public alarm); (2) those where the primary purpose of the Act is to maintain an efficient system of justice or enforcement, see, eg Criminal Justice and Public Order Act 1994, s 51 (which criminalises threats made to witnesses or jurors during an investigation or court proceedings); (3) those where the primary purpose of the Act is to protect those with an interest in property from threatening behaviour, see, eg Administration of Justice Act 1970, s 40 (which protects debtors from unlawful harassment), Protection from Eviction Act 1977, s 1 (which protects an occupier from unlawful eviction and harassment), Criminal Law Act 1977, s 6 (which criminalises the use of violence for securing entry to property without lawful authority); (4) those where the threat is directed at property rather than a person, see, eg Criminal Damage Act 1971, ss 1 and 2; (5) those where the offence falls outside our general terms of reference for this project, see, eg Internationally Protected Persons Act 1978, s 1(3); Aviation Security Act 1982, s 1; Taking of Hostages Act 1982, s 1; Nuclear Materials (Offences) Act 1983, s 2(3); Nuclear Materials (Offences) Act 1983, s 2(4); Aviation and Maritime Security Act 1990, s 13(1); Aviation and Maritime Security Act 1990, s 13(2).

7.7 Those who make threats may also be prosecuted under legislation we discuss in detail elsewhere in this Report, including:

(1) sections 2, 2A, 4 and 4A of the Protection from Harassment Act 1997 ("PHA 1997"), under which those who pursue a course of conduct which amounts to harassment or stalking of others, or putting them in fear of violence, may be prosecuted;

(2) section 1 of the Malicious Communications Act 1988 ("MCA 1988") which criminalises any person who conveys a threat electronically or by letter; and

(3) section 127(1) of the Communications Act 2003 ("CA 2003"), under which a person will be guilty of an offence if they send a menacing message via a public electronic communications network.

7.8 In Chapter 10 we also discuss the specific concern of threatening to reveal private sexual imagery of another without consent, which is currently not a specific threat offence.

Problems with threat offences in the current law generally

7.9 It has been said that there is "disappointingly little coherence in English law's approach to threat offences".[3] Alldridge recommended in the 1990s that there should be a "wholesale review of the criminal law of threats" suggesting that, "for too long threats offences have been allowed to develop in an entirely ad hoc manner without reference to any governing rationale, or to considerations of consistency and coherence and without reference to any other offences of causing fear".[4]

7.10 Alldridge's principal criticisms of the current law were first, that there is little analysis of the basis on which threats offences are made criminal at all, and secondly, that when threats are criminalised, there is no coherence in the approach. So, for example, in his view it was illogical to criminalise a threat to property, "while threats to cause bodily harm short of death, which do not have the immediacy of assault and are not otherwise criminal are not".[5]

7.11 In 2015, we reviewed the OAPA 1861 offences and made recommendations for reform.[6] Those recommendations included, for example, that the offence of threatening to kill should be expanded to include an offence of threatening to cause serious injury or to rape any person.

7.12 In this Report, we do not discuss general proposals for reforming the law relating to threats. Instead, we focus on the particular issues that arise in the criminalisation of online threats.

---

3 D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (15th ed, 2018) p 1006. This passage in the 13th edition was cited with approval by Lord Judge CJ in *Chambers v DPP* [2012] EWHC 2157 (Admin) at [29].

4 P Alldridge, "Threats Offences – A Case for Reform" [1994] *Criminal Law Review* 176.

5 P Alldridge, "Threats Offences – A Case for Reform" [1994] *Criminal Law Review* 176. (Note that this was prior to the Protection from Harassment Act 1997).

6 Reform of Offences Against the Person (2015) Law Com No 361.

Definition of threats adopted by social media companies

7.13 As highlighted in Chapter 2, the day to day control of abusive and offensive behaviour online in practice often falls to the discretion of the social media platforms. Although outside our terms of reference for this project, this is part of the context in which the discussion of the criminal law should be understood.

7.14 Social media companies have their own corporate definitions of what constitutes threatening behaviour on their platform. For example, Twitter forbids its users from "mak[ing] specific threats of violence or wish[ing] for the serious physical harm, death, or disease of an individual or group of people".[7] The platform defines a violent threat as "explicit statements of one's intent to kill or inflict serious physical harm against another person. This includes, but is not limited to, threatening to murder someone, sexually assault someone, break someone's bones, and/or commit any other violent act that may result in someone's death or serious injury".

7.15 Twitter excludes from its "violent threats and glorification of violence" policy "wishing or hoping that someone experiences serious physical harm, making vague threats, or threatening less serious forms of physical harm". Rather, it says that type of threatening conduct might instead be covered by its "abusive behaviour and hateful conduct policies".[8]

7.16 In contrast, Facebook, once it has established that a threat has been made, takes a wider contextual view to determine whether it is "credible". Facebook's community standards suggest that this approach is justified because "people commonly express disdain or disagreement by threatening or calling for violence in facetious and non-serious ways".[9] The platform uses this rationale for trying to "consider the language, context and details in order to distinguish casual statements from content that constitutes a credible threat to public or personal safety". In determining whether or not a threat is credible, the platform also looks at information relating to the victim including "a targeted person's public visibility and vulnerability".[10]

THE CRIMINAL LAW GOVERNING RELEVANT THREAT OFFENCES

Offence of threatening to kill

7.17 Threatening to kill another person is an offence under section 16 of the OAPA 1861. Section 16 provides that:

> A person who without lawful excuse makes to another a threat, intending that that other would fear it would be carried out, to kill that other or a third person shall be

---

7 Twitter, *Violent threats and glorification of violence*, available at https://help.twitter.com/en/rules-and-policies/violent-threats-glorification.

8 Twitter, *Violent threats and glorification of violence*, available at https://help.twitter.com/en/rules-and-policies/violent-threats-glorification.

9 Facebook, *Credible violence*, available at https://en-gb.facebook.com/communitystandards/violence_criminal_behavior/credible_violence.

10 Facebook, *Credible violence*, available at https://en-gb.facebook.com/communitystandards/violence_criminal_behavior/credible_violence.

guilty of an offence and liable on conviction on indictment to imprisonment for a term not exceeding 10 years.

7.18 There is no requirement that the threatened person should ever become aware of the threat to kill him or her, or any other person; it is sufficient that the defendant made the threat.[11] The threat does not have to be express; an implied threat would be enough.[12]

7.19 It does not matter whether the defendant actually intended to carry out the threat to kill or not. The fault element of the crime is satisfied if the defendant intends the person who hears the threat to "fear it would be carried out". The person who hears the threat need not be certain it will be carried out and it seems that a conditional threat, such as "if you don't do such and such I will kill you", would suffice.

7.20 The threat to kill does not need to be immediate, and it does not need to be made by a person within the jurisdiction. For example, a threat made from abroad and received in England or Wales via email would be enough to constitute the offence.[13]

7.21 A person commits the offence only if the threat is one which would be carried out by the defendant, or at least under his or her instructions.

7.22 For over a century, the law limited the offence such that it could only be committed by sending a threat in a letter.[14] Now, it can be committed by any means, both online and offline. Examples of cases resulting in conviction include a threat made by telephone[15] and a threat to kill made via WhatsApp and Snapchat.[16]

7.23 The relevant Crown Prosecution Service ("CPS") Charging Standard notes that this charge can be difficult to prove and that it should be reserved for more serious cases. Prosecutors are encouraged to consider an alternative charge under section 4 of the POA 1986 if there is any doubt about whether the threat carries the necessary intent.[17] Even with this advice, prosecution success rates remain relatively low. Ministry of

---

11 In *R v Tait* [1990] 1 QB 290, the Court held that a threat to kill a foetus is not a threat to kill as the foetus is not another person distinct from its mother. However, the Court accepted the reasoning in *Shephard* [1919] 2 KB 125; (1920) 14 Cr App R 26, that an unambiguous threat to kill the child after it was born would have been an offence. See also *R v Donovan* [2009] EWCA Crim 1258, where the defendant described his intention to kill a member of his extended family to a member of staff whilst incarcerated.

12 See *R v Solanke* (1970) 54 Cr App R 20, where the Court of Appeal held that it was "obviously inarguable" to say that an implied threat to kill was not covered by section 16 of the OAPA 1861.

13 See *R v Mawji* [2003] EWCA Crim 3067, where the defendant was arrested on his return to the United Kingdom and convicted of threatening to kill his wife after emailing her from another country to say "Hi bitch, don't think you are safe in the UK I am going to kill you I will make sure I get my hands on you, your loving husband Riz [sic]".

14 The requirements of the offence were also very different historically. For example, until 1977, there was no requirement of intent to cause fear and the fault element was expressed as "maliciously".

15 *R v Williams* (1987) 84 Cr App R 299.

16 *R v Furmage* [2018] EWCA Crim 433. Messages included, "if you make me pull my gun out, I will fucking murder you", accompanied by a picture of a firearm on the defendant's sofa.

17 Crown Prosecution Service*, Legal Guidance: Offences Against the Person, incorporating the Charging Standard* (13 June 2018), available at https://www.cps.gov.uk/legal-guidance/offences-against-person-incorporating-charging-standard.

Justice data indicate that 1277 threat to kill cases were prosecuted in 2017, of which fewer than half resulted in convictions. Of those who were convicted and received a sentence of imprisonment, the median length of sentence was 17.8 months. In *R v Furmage,*[18] where a young offender made threats, over social media, to kill a former girlfriend and her friend, he received a sentence of four years' detention in a young offenders' institution.[19]

7.24 There are no statistics available to show whether threats to kill are predominantly made offline or online, or to indicate whether there has been an increase in this type of offending behaviour, as use of social media has grown in popularity and reach.

7.25 Prosecuting a threat to kill made online raises some questions about the ways in which a communication could be said to be made "to another" online. It also raises questions about whether communication online is in some way different to communication in the offline world.

Offence of assault

7.26 An assault is committed when a person intentionally or recklessly causes another to apprehend immediate and unlawful violence.[20]

7.27 No actual physical violence is required; the victim's apprehension of violence is enough. "Apprehend" is wider than "fear" in that the victim need not feel frightened.

7.28 The victim's apprehension can arise through the defendant's words alone.[21] The offence of assault can therefore be committed by the sending of threatening letters[22] or, by extension, via email, text message and posts on social media platforms.

7.29 In *R v Ireland*[23] the defendant had been convicted of assault occasioning actual bodily harm after making a series of silent phone calls to three women. The defendant appealed his conviction. On appeal, the Court of Appeal warned of the need to ensure that cases were interpreted in line with technological advancement, saying:

> The early cases predate the invention of the telephone. We must apply the law to conditions as they are in the 20th century.[24]

---

18 [2018] EWCA Crim 433.

19 *R v Furmage* [2018] EWCA Crim 433 at [16].

20 See Criminal Justice Act 1988, s 39. For more on the difference between assault and battery (where unlawful force is in fact applied) see Reform of Offences Against the Person (2015) Law Com No 361.

21 *R v Burstow* [1997] 1 Cr App R 144*; R v Ireland* [1997] UKHL 34; [1998] AC 147.

22 The Court of Appeal in *R v Constanza* [1997] 2 Cr App R 492 rejected the "dubious foundation" in the earlier authority (*Meade and Belt's Case* (1823) 1 Lewin 184) that words alone were incapable of amounting to an assault.

23 [1997] QB 114.

24 *R v Burstow* [1996] 3 WLR 350; *R v Ireland* [1997] QB 114 at 119, per Swinton Thomas LJ.

7.30 When agreeing on appeal that repeated telephone calls of a menacing nature were capable of constituting an assault, the House of Lords emphasised the need for the victim to apprehend immediate (or at least imminent) violence. If the victim did not fear immediate physical violence, perhaps instead fearing the receipt of further phone calls, that would be insufficient to make out the offence. Similarly, if the victim was not aware of the threat at all, for example, because they were not present to answer the phone, or subsequently picked up a voicemail message weeks later, then there was no assault.

7.31 The timing of any threat of violence is therefore important. The apprehension must be that violence will be carried out immediately. If it is clear to the potential victim that the defendant can do nothing to harm them in the immediate future, then the offence is not committed. Although, as Blackstone's puts it, the concept of immediacy has been interpreted with "some flexibility" by the courts.[25] For example, in *Smith v Chief Superintendent, Woking Police Station*[26] a threat of violence was considered to be immediate when the defendant was outside the victim's home but would have needed to force entry before he could inflict physical harm. The focus should, nevertheless, be on whether there is apprehension of immediate violence; not whether there is immediate apprehension of violence.

7.32 Conditional words in a threat can negate an assault. Famously, the 17th century authority *Tuberville v Savage*[27] held that placing a hand on one's sword (ordinarily capable of amounting to assault) was negated by the words "if it were not assize time, I would not take such language from you". On the other hand, it is clear that a threat need not be explicit to constitute an assault, so long as it causes the victim to apprehend the infliction of immediate violence.[28]

7.33 This raises interesting questions about how far someone can exculpate online behaviour which might otherwise constitute an assault by caveating it with conditional words. We have heard that menacing "non-threats" are a common form of abuse on the internet. For example, a tweet reading "I'd love to rape you but you're such a filthy slut you'd probably allow me to do as I please, so it wouldn't be rape".

7.34 It seems clear that the internet can provide the medium for committing an assault. A message on any platform which caused apprehension of immediate violence could very well constitute the offence; for example, a WhatsApp message which read "you have not paid your drug debt and I am coming for you now". However, the offence is rooted in imminence. In many instances this may be difficult to prove, particularly given the fact that many online messages may be conveyed between a defendant and victim who are geographically distant, or where the identity of the sender is not known. The offence was also not designed to capture the sort of anxiety caused by multiple and sustained threats which may lead to psychiatric or psychological harm. It was this kind of harm that many who attended our stakeholders' experiences event described.

---

25 D Ormerod and D Perry (eds), *Blackstone's Criminal Practice 2019*, para B2.6.

26 (1983) 76 Cr App R 234.

27 (1669) 1 Mod 3.

28 *R v Ireland* [1997] UKHL 34; [1998] AC 147.

Public Order Act 1986 offences

7.35 The POA 1986 contains a range of offences which can apply to threats of violence made online in some circumstances. In this Chapter, we discuss the offences contained in sections 4, 4A and 5 of the POA 1986 and their applicability to online offences.

7.36 All three offences have the significant limitation that they cannot be committed if the perpetrator and the victim are both inside a "dwelling", or the perpetrator was inside a dwelling and "had no reason to believe that the words or behaviour used, or the writing, sign or other visible representation displayed, would be heard or seen by a person outside that or any other dwelling".[29]

7.37 It is, of course, common for online interaction to take place between people in their homes. This requirement may arbitrarily restrict the usefulness of these offences in addressing threatening behaviour online.

7.38 Further, the existence of the "dwellings exemption" reflects the clear intent of the lawmakers that public order offences should, as the name suggests, be criminalised when committed in public spaces. As Williams has asserted, the law of public order was a compromise which sought to balance the "competing demands of freedom of speech and assembly on the one hand and the preservation of the Queen's Peace on the other".[30] Stannard has observed that "the main rationale of these offences is said to be the need to preserve public confidence in the stability of society".[31]

7.39 Below we acknowledge some of the criticisms made of the application of public order offences to online communications.

Section 4 of the Public Order Act 1986: fear or provocation of violence

7.40 Under section 4 a person is guilty of an offence if they:

(1) use towards another person threatening, abusive or insulting words or behaviour; or

(2) distribute or display to another person any writing, sign or other visible representation which is threatening, abusive or insulting;

with intent to cause that person to believe that immediate unlawful violence will be used against them or another by any person, or to provoke the immediate use of unlawful violence by that person or whereby that person is likely to believe that such violence will be used or it is likely that such violence will be provoked.

---

29 A "dwelling" is defined in section 8 of the Public Order Act 1986 as being "any part of a structure occupied as a person's home or as other living accommodation" with "structure" capable of encompassing a tent, caravan, vehicle or vessel or other movable or temporary structure. A private garden would not generally be part of a dwelling for the purposes of public order offences, so for example, a section 5 offence could be committed when words were directed from one private garden to a person in another private garden.

30 D Williams, *Keeping the Peace: The Police and Public Order* (1967) p 9, as quoted in I Channing, *The Police and the Expansion of Public Order Law in Britain, 1829-2014* (2015) p 1.

31 J E Stannard, "Sticks, Stones and Words: Emotional Harm and the English Criminal Law" (2010) 74(6) *Journal of Criminal Law* 533, 543.

7.41 By requiring the offence to be committed "towards another", section 4 is the only public order offence which requires a specific victim.[32]

7.42 In *Atkin v DPP*[33] the Divisional Court considered a conviction for a section 4 offence where a threat to a bailiff waiting in a car was relayed to him by a Customs and Excise Officer who had spoken to the defendant nearby. The conviction was quashed on the basis that the threat had not been made in the presence of or addressed to the person threatened.

7.43 The alternative offence under section 4(1)(b) criminalises a "distribution" or "display" of a threat. It has been suggested that "the term 'display' appears to connote an element of public showing".[34] Under section 4(2) "no offence is committed where … the writing or sign or other visible representation is distributed or displayed, by a person inside a dwelling and the other person is also inside that or another dwelling".

7.44 The immediacy of the feared unlawful violence is a question of fact. In *R v Horseferry Road Metropolitan Stipendiary Magistrates ex parte Siadatan*[35] the Divisional Court gave a provisional view on the word "immediate", noting that

> it does not mean 'instantaneous'; … a relatively short time interval may elapse between the act which is threatening, abusive or insulting and the unlawful violence. 'Immediate' connotes proximity in time and proximity in causation; that it is likely that violence will result within a relatively short period of time and without any other intervening occurrence.[36]

7.45 In *DPP v Ramos*,[37] the sender of two letters to an Asian community advice centre threatening the start of a bombing campaign and the murder of the recipient was held to have made a threat of immediate violence contrary to section 4(1)(b). The Divisional Court held on appeal that "it was the state of mind of the victim which was crucial rather than the statistical risk of violence actually occurring within a short space of time".[38] Provided, therefore, the victim believed and was likely to believe that something could happen at any time, there was a case to answer.

7.46 This decision has been criticised, most notably by Sir John Smith QC, who observed:

> it is easy to understand that the recipients of the letters were "immediately concerned for their own and others safety" as the magistrate found. It is less easy to see that it

---

32 However, it seems it is not necessary for that person to be called to give evidence see, eg *Swanston v DPP* (1997) 161 JP 203 where the prosecution relied on evidence from a bystander.

33 (1989) 89 Cr App R 199.

34 HHJ P Thornton and others, *The Law of Public Order and Protest* (2010), p 33.

35 [1991] 1 QB 260.

36 [1991] 1 QB 260 at 269. See also, *Valentine v DPP* [1997] COD 339, where the Divisional Court followed the decision in *Horseferry Road Metropolitan Stipendiary Magistrates Court ex parte Siadatan*, and held that the defendant's threat to burn down his neighbour's house when the victim was next on duty was an immediate one on the basis that the victim's next shift could have been that evening.

37 [2000] *Criminal Law Review* 768.

38 *DPP v Ramos* [2000] All ER (D) 544 at [10].

was open to him to infer than they feared immediate violence …[this] is very far removed from the traditional examples of assault where the victim flinches from the upraised first, the drawn sword or the charging horse.[39]

7.47 The question of what is "threatening, abusive or insulting" is also a question of fact. Lord Reid said in *Brutus v Cozens*:[40]

> Vigorous and it may be distasteful or unmannerly speech or behaviour is permitted so long as it does not go beyond any of these limits. It must not be threatening. It must not be abusive. It must not be insulting. I see no reason why any of these should be construed as having a specially wide or specially narrow meaning. They are easily recognisable by the ordinary man.[41]

7.48 The fault element of the offence under section 4 of the POA 1986 has two parts, both of which must be met. The first is that the defendant either intends his or her words or behaviour to be threatening, or is aware that they may be.[42] The second requires some anticipation of the reaction to the threat and can be fulfilled in four different ways:[43]

(1) The accused intends the person against whom the conduct is directed to believe that immediate unlawful violence will be used against them or another by any person. It is immaterial whether the other person actually believed that the violence would happen.

For example, Brian is among the crowd at a festival. He spots Anna in the crowd and sends her a text saying he can see her, and is going to attack her.[44]

(2) The accused intends to provoke the immediate use of unlawful violence by the person against whom the threat is directed or another.

For example, Anna and Craig are part of a WhatsApp group. Anna sends Craig a message suggesting they attack Brian. Brian is with Craig at the time and sees the message appear on Craig's phone.

(3) The person against whom the words, behaviour, distribution or display are directed is likely to believe such violence will be used.

(4) It was likely such violence would be provoked.

For example, Anna knows that Brian has recently been tried for a child sex offence and was found not guilty, she believes on a "technicality". She posts a

---

39 JC Smith, "Public order offence: respondent sending letters stating an intention to arrange a bombing hate campaign" [2000] *Criminal Law Review* 768, p 769.

40 [1973] AC 854 at 862.

41 *Brutus v Cozens* [1973] AC 854 at 862.

42 Public Order Act 1986, s 6(3).

43 Public Order Act 1986 s 4(1). This analysis is taken from HHJ Thornton and others, *The Law of Public Order and Protest* (2010), p 33.

44 If Anna apprehends immediate violence as a result of the text, it will also constitute an assault.

message on the Facebook page of a known violent "paedophile hunter" group, telling the group about Brian and suggesting that he deserves to be "sorted out".[45]

7.49 In all four circumstances the defendant will only be guilty under section 4 of the POA 1986, if he or she intends the words or behaviour or the writing, sign or other visible representation, to be threatening, abusive or insulting or is aware that they may be threatening, abusive or insulting.[46]

Section 4A of the Public Order Act 1986: intentional harassment, alarm or distress

7.50 Under section 4A of the POA 1986 a person is guilty of an offence if, with intent to cause a person harassment, alarm or distress they (a) use threatening, abusive or insulting words or behaviour or disorderly behaviour; or (b) display any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

7.51 The offence is one of specific intent.

7.52 The High Court has described the words harassment, alarm and distress as being "relatively strong words" and clarified that "distress" requires "real emotional disturbance and upset".[47]

7.53 There must be a link between what the defendant does and the harassment, alarm or distress experienced by the other person, but the material need not be in the public domain by the time it causes the reaction. For example, in *S v DPP*[48] material was displayed on an animal rights website which showed the complainant security guard outside his place of work at an animal testing company. The defendant added a speech bubble to the image and commentary which suggested that the guard had been convicted of violence in the past, which was untrue. The guard did not see the image while it was posted online, and it had been removed from the web by the time the police, who had captured a copy of it, showed it to him. Although the image no longer existed in the online sphere, the fact that it had been captured and subsequently shown to the victim would suffice. It was irrelevant that the harassment, alarm or distress crystallised five months after the image had been posted.

7.54 Mr Justice Walker suggested that the person alarmed or distressed did not even need to see the writing or image for the offence to be made out:

> Suppose that the police, rather than showing the complainant an image which had been posted on the World Wide Web, simply told that person details of what had happened. If the posting of the material on the World Wide Web had been done by the defendant with intent to cause a person harassment, alarm or distress, and it did indeed cause harassment, alarm or distress, albeit only because the person in

---

45 Anna may also be guilty of communications offences in this example.

46 Public Order Act 1986, s 6(3).

47 *R(R) v DPP* [2006] EWHC 1375 (Admin); (2006) 170 JP 661 at [12].

48 [2008] EWHC 438 (Admin); [2008] 1 WLR 2847.

question was informed by another, I see no objection for that reason only to the defendant being found guilty of the offence.[49]

Section 5 of the Public Order Act 1986: harassment, alarm or distress

7.55 Under section 5 of the POA 1986 a person is guilty of an offence if they (a) use threatening or abusive words or behaviour, or disorderly behaviour; or (b) display any writing, sign or other visible representation which is threatening or abusive, within the hearing or sight of a person likely to be caused harassment, alarm or distress thereby.

7.56 Prior to 2013, the offence also extended to "insulting" words, however this language was removed following concern that this extended the reach of the offence too far.[50]

7.57 The offence does not require any violent behaviour or indeed the threat of violence.

7.58 It is also not necessary for the prosecution to prove any intention to cause harassment, alarm or distress. Section 6(4) of the Act sets out the fault element required to commit the offence, namely either an intention that the words or behaviour or displays are threatening or abusive, or an awareness that they may be threatening and abusive, or awareness that it may be disorderly.

7.59 It is also not necessary to prove that anyone has actually been caused harassment, alarm or distress; it is enough that someone was able to see or hear the threat and was likely to be caused harassment, alarm or distress by it. The prosecution does not need to show that the person in question actually saw or heard the threat.[51]

7.60 There are two ways in which a section 5 offence may potentially be committed online: "using" threatening or abusive words or behaviour, or by "displaying" threatening or abusive words or signs.

7.61 In *Chappell v DPP*,[52] the Divisional Court agreed that the posting of a letter through a box, where the writing containing the abusive or insulting words was inside and was concealed by an envelope, could not on any sensible reading amount to a "display" in the ordinary sense of that word. This raises the question of the extent to which the web and applications operating over the internet are public spaces where abusive and offensive messages are put on "display". A message posted for the world at large on Facebook is probably "on display", but this may not be as straightforward if the message was sent using a private encrypted messaging service.

7.62 Nevertheless, there are a number of reasons why this may not be an appropriate charge where the offending was perpetrated over the internet. First, the "dwelling exemption" could complicate prosecutions, as it would require the prosecution to prove that the messages were not sent and received inside dwellings. Secondly, there are alternative

---

49 [2008] EWHC 438 (Admin); [2008] 1 WLR 2847 at [15].

50 Crime and Courts Act 2013, s 57. See also P Strickland and D Douse, *"Insulting words or behaviour": Section 5 of the Public Order Act 1986* (Standard Note SN/HA/560, 15 January 2013), available at http://researchbriefings.files.parliament.uk/documents/SN05760/SN05760.pdf.

51 *Taylor v DPP* [2006] EWHC 1202 (Admin); (2006) 170 JP 485.

52 (1988) 89 Cr App R 82.

and more specific offences designed to deal with such threatening and abusive behaviour, which we discuss further in Chapters 4 and 8. Thirdly, it is arguable that the words "within the sight or hearing of a person likely to be caused harassment or distress" imply that the defendant must be present when that person views (or could have viewed) the offending material. It is not clear whether both the defendant and victim being online simultaneously would meet the requirement, but Bakalis has suggested that it rules section 5 out in application to threatening, abusive or disorderly behaviour online.[53]

Criticisms of the application of public order offences to abusive and offensive communications online

7.63 Criticism of the general application of public order offences to online communications reflects two prevailing themes:

(1) that public order offences were not designed for an online space; and

(2) that applying these offences adds to the confusion caused by overlapping legislation.

7.64 The dwelling exception reflects the genesis of the public order offences which are, as Rowbottom has observed, "primarily about standards of behaviour in public".[54]

7.65 The law of public order has been described as being "often made to reflect its time".[55] The statute law has seemingly developed by responding to signal events in the offline world, resulting in a transition from common law to statute-based offences and subsequent legislative amendments. These events have included the fascist marches of the 1930s, resulting in the Public Order Act 1936, and the Southall riots of 1979, Brixton riots of 1981 and miners' strike in the 1980s, which preceded the Public Order Act 1986. At the second reading of the Bill, the need to safeguard public order, protect the public and for "quiet streets and a peaceful framework for our public lives" were all emphasised.[56]

7.66 This emphasis on public behaviour has led some academics to be critical of the expansion of public order to encompass communications sent online, which the sender may think of as semi private or being made outside a public space. As Rowbottom has observed:

> The law seeks to manage the competing rights and interests of people sharing public spaces. Speech in public places is harder for people to avoid and face-to-face communication can have different impact on the listener. That is what makes public

---

53 C Bakalis, "Rethinking cyberhate laws, Information & Communications Technology Law" (2018) 27(1) *Information & Communications Technology Law* 86, p 94. Bakalis notes that while sections 4 and 4A of the Public Order Act 1986 can in theory be used for online conduct, their usefulness is limited.

54 J Rowbottom, "To rant, vent and converse: protecting low level digital speech" 71(2) *The Cambridge Law Journal* 355, p 361.

55 HHJ P Thornton and others, *The Law of Public Order and Protest* (2010) p v.

56 *Hansard* (HC), 13 January 1986, vol 89, col 795 (Mr Douglas Hurd, Secretary of State for the Home Department).

> protest so powerful, but also what makes some legal control necessary. Public order laws were initially drafted to exclude certain private communications, such as a domestic row or phone call from one house to another. … The public order controls on expression primarily target activities "on the ground", in which there is physical proximity between the speaker and listener.[57]

7.67 Haralambous and Geach have argued that the section 5 and 4A offences are of "questionable value for the social networking age", contributing "to the issues of uncertainty and inaccessibility of the overall legislative framework".[58]

Protection from harassment

7.68 For detailed discussion of harassment offences, see Chapter 8.

7.69 When prosecuting threatening behaviour, the PHA 1997 is both more restrictive and wider than the POA 1986. It is narrower because in order to bring a successful prosecution under the PHA 1997, the prosecutor must prove that the defendant carried out a "course of conduct".[59] In other words, there must be evidence of two or more examples of the offending behaviour. In the words of Lord Hoffmann this provision is a safety net as "parliament was conscious that it might not be in the public interest to allow the law to be set in motion for one boorish incident".[60] In contrast, the POA 1986 can apply to a single act.

7.70 However, the POA 1986 requires the defendant's conduct – words and behaviour – to be threatening, abusive or insulting or disorderly. The PHA 1997 does not define harassment and the authorities suggest that it would encompass less serious individual incidents of behaviour which, provided they amount to an oppressive and unreasonable course of conduct, causes "annoyance or worry" and alarm and distress.[61]

7.71 Commentators have argued that:

> [the] conflict between these two different pieces of legislation means that there is obvious confusion and lack of cohesive legislation … this creates practical difficulties for prosecutors who need to be able to determine which charge is the most appropriate response to the alleged act and its consequences … the present overall legislative framework is inaccessible and uncertain due to the range of offences which could apply depending on the facts.[62]

---

57 J Rowbottom, "To rant, vent and converse: protecting low level digital speech" 71(2) *The Cambridge Law Journal* 355, p 361.

58 N Haralambous and N Geach, "Regulating Harassment: Is the Law Fit for the Social Networking Age?" (2009) 73 *Journal of Criminal Law* 241, p 256.

59 Protection from Harassment Act 1997, s 1.

60 See *Wainwright v Home Office* [2004] 2 AC 406 at [46].

61 See *DPP v Ramsdale* [2001] EWHC Admin 106 at [16]; and *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233; [2002] Entertainment and Media Law Reports 4 at [30].

62 N Haralambous and N Geach, "Online Harassment and Public Dis-order" (2010) 174 (27) *Criminal Law & Justice Weekly* 409, p 411.

7.72 In Chapter 8 we discuss the particular challenges that arise in relation to offences under the PHA 1997 when applied to online communication.

Communications offences and threats

7.73 In Chapter 4 we analysed the specific communications offences under section 127(1)(a) of the CA 2003 and section 1 of the MCA 1988. Both of those provisions contain threats offences. For example, section 127 makes it an offence to send via a public electronic communications network a message or other matter of a menacing character. Section 1 of the MCA 1988 makes it an offence to send to another person a letter, electronic communication or article of any description which conveys a threat.

7.74 Examples of recent cases involving threatening behaviour being prosecuted under the malicious communication legislation include *Att-Gen's Ref 2017 Re Watts*[63] where the defendant admitted sending a series of five offensive and violent threats via text message over a 30 minute period.[64] He then ran to the victim's property and filmed himself shouting threats and kicking the front door. He received a one-month sentence of imprisonment for the communications offence, which ran consecutively to a 30 month sentence for a separate threat to kill.

7.75 The communications offences are discussed in more detail in Chapter 4, which sets out, for example, the fault element required to commit the offence. For the purpose of analysing the criminal law which protects victims from threats made online, the offences are interesting because, in applying the law, the courts have been required to address how the words of the statute should be interpreted in light of online behaviours.

7.76 For example, the meaning of "menacing" was considered in *Chambers v DPP.*[65] The defendant had posted a tweet online which read:

> Crap! Robin Hood airport is closed. You've got a week and a bit to get your shit together otherwise I'm blowing the airport sky high.[66]

7.77 The High Court allowed his appeal against conviction on the basis that this tweet did not constitute or include a message of a menacing character. Elsewhere in the judgment, the Court concluded that

> if the person or persons who receive or read it, or may reasonably be expected to receive or read it would brush it aside as a silly joke, or a joke in bad taste, or empty bombastic or ridiculous banter, then it would be a contradiction in terms to describe it as a message of a menacing character.[67]

---

63 [2017] EWCA Crim 1009; [2017] 2 Cr App R (S) 52.

64 Another option in this context may have been to prosecute an offence under the Protection from Harassment Act 1997, as the series of text messages may have amounted to a "course of conduct" for the purposes of these offences. We discuss harassment and stalking offences further in Chapter 8.

65 [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833.

66 [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [12].

67 [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [29].

7.78 In considering the definition of "menace", the High Court were told that the word is defined in the shorter Oxford English Dictionary as "a thing threatening danger or catastrophe; a dangerous or obnoxious thing or person; a great inconvenience" and that to use menace as a verb meant to "utter menaces; be threatening".[68]

7.79 The Court felt that in order to have a menacing quality the message would need to be one which would "create fear or apprehension in those to whom it is communicated, or who may reasonably [be] expected to see it".[69] In this case the message did not have those characteristics. Even if it had, the Court went on to say that the fault element of the case required the offender to have intended that the message should be of a menacing character or be aware of, or to have recognised the risk at the time of sending the message, that it may create fear or apprehension in any reasonable member of the public who sees it.

7.80 The Lord Chief Justice stated:

> 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 [section 127 of the Communications Act 2003].[70]

7.81 The approach of the Court in *Chambers*[71] illustrates the importance of context in deciding whether or not a message is of menacing character. In that case, the Court took into account the fact that the airport staff did not take the threat seriously, nor did any of the readers of the tweet. They reported it only as a matter of procedure, rather than of serious concern, and the Yorkshire police did not take immediate and urgent action in response. This, taken with the actual content of the tweet, the fact that it was not directed to any particular member of staff, that Chambers posted it using his real identity, and the fact the threat was widely accessible, were all characteristics inconsistent with a credible threat.

7.82 This highlights the blurring of public and private communication in the online environment. Chambers may have been writing primarily for a single person, or a small group of followers, confident that they would interpret his intention. The platform he chose was, however, a public one, and his message was capable of being viewed by anyone with access to Twitter. While even to a wider audience Chambers' tweet was fairly clearly not a threat, messages and modes of communication which would be understood as more or less innocent within one cultural context, might seem profoundly threatening when they reach outside it.

7.83 Further, there can be difficulty in inferring tone and intent from an online written or visual communication. Unlike a face to face communication, there is no accompanying tone, volume or gesture, and no visible reactions from others (such as cowering or hiding). It can be difficult, then, to infer from an online communication whether, for example, a

---

68 [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [30].

69 [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [30].

70 [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833 at [28].

71 *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833.

threat is sincere, or whether a person intends to be menacing or grossly offensive, rather than humorous. The now widespread use of "emojis" can further complicate interpretation. For example, would an otherwise threatening message followed by "wink" emoji make it any less threatening?

7.84 In *Karsten v Wood Green Crown Court*[72] the Court followed the approach in *Chambers* noting that in the relevant context (a background voice in an anonymous phone call) the words "Ask him if he's Jewish. Ask him if he's eating kosher" was a "nasty, malicious antisemitic comment of which the appellant should be thoroughly ashamed", but it was not menacing.[73]

7.85 Article 10 considerations and CPS guidelines[74] also caution that prosecution must be in the public interest as well as necessary and proportionate. We outline these guidelines in more detail in Chapter 4.

Particular challenges of prosecuting threats offences committed online

7.86 When assessing the challenges that threatening behaviour online presents to the current criminal law, it is necessary to reflect on some of the qualities of online communications. It is also necessary to consider the ways in which online threats can be similar to, and different from, threats in the offline world.

7.87 Online communication allows threats to be communicated quickly, over long distances, often directly from one person's place of residence into another's. It also blurs our conception of public and private spaces. A person online can be simultaneously both alone in the privacy of their own home, and communicating publicly in real time with numerous people.

7.88 It has also enabled new forms of threatening behaviour to emerge where the online threats spill into offline behaviour, for example, the sharing of the victim's address (a practice known as "doxing") or encouraging people to collectively "dogpile" into a victim's social media accounts to make conditional threats. For example, some female MPs have reported receiving hundreds of messages from individual social media accounts asserting that the sender had no intention of raping them.

7.89 Victims have recounted the ways in which receiving online threats has impacted on their personal and professional lives. Laura Bates described to Amnesty International her experience of receiving more than 200 threats a day online:

> The psychological impact of reading through someone's really graphic thoughts about raping and murdering you is not necessarily acknowledged. You could be sitting at

---

72 [2014] EWHC 2900 (Admin).

73 The trial had also involved an allegation that the phrase "filthy jew" was uttered. The Court noted that this phrase was clearly grossly offensive, but there was insufficient evidence to connect the defendant to this statement: *Karsten v Wood Green Crown Court* [2014] EWHC 2900 (Admin) at [6] to [7].

74 See Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (21 August 2018), available at https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media.

home in your living room, outside of working hours, and suddenly someone is able to send you an incredibly graphic rape threat right into the palm of your hand.[75]

7.90 She has further written that:

> If you're on the receiving end of hundreds of long, detailed, graphic threats, you can't help wondering whether just one person might follow through. And when you've received a detailed rape threat with an exact time and date in it, it's very hard not to start looking at your watch as the hour draws near, no matter how rational you are.[76]

7.91 Bates' words convey much of the same sense of apprehension and fear that Lord Steyn described in *Ireland*[77] when the House of Lords justified the interpretation of the offence of common assault to cover silent calls:

> It is easy to understand the terrifying effect of a campaign of telephone calls at night by a silent caller to a woman living on her own. It would be natural for the victim to regard the calls as menacing. What may heighten her fear is that she will not know what the caller may do next. The spectre of the caller arriving at her doorstep bent on inflicting personal violence on her may come to dominate her thinking. After all, as a matter of common sense, what else would she be terrified about? The victim may suffer psychiatric illness such as anxiety neurosis or acute depression. Harassment of women by repeated silent telephone calls, accompanied on occasions by heavy breathing, is apparently a significant social problem. That the criminal law should be able to deal with this problem, and so far as is practicable, afford effective protection to victims is self evident.[78]

7.92 Statistics show that online threats do result in offline physical violence. Women's Aid, a domestic violence charity, conducted research into online domestic abuse: 50% of respondents reported that the online abuse they experienced also involved direct threats against them or someone they knew. Nearly a third of respondents who had received threats stated that when online threats had been made by a partner or ex-partner they were carried out.[79]

7.93 In this section we consider some of the challenges which arise when taking the "patchwork" of threats provisions in the English law and attempting to apply them to offences committed online rather than offline.

---

75 As quoted in *Amnesty reveals alarming impact of online abuse against women* (20 November 2017), available at https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/.

76 L Bates, *Eight things not to say to someone facing online abuse* (19 April 2016), available at https://www.theguardian.com/lifeandstyle/2016/apr/19/eight-things-not-to-say-to-someone-facing-online-abuse; see also L Bates, *Misogynation: The True Scale of Sexism* (2018).

77 *R v Ireland* [1997] UKHL 34; [1998] AC 147.

78 *R v Ireland* [1997] UKHL 34; [1998] AC 147, p 152.

79 See All-Party Parliamentary Group on Domestic Violence and Women's Aid, *Tackling domestic abuse in a digital age* (February 2017), p 9, available at https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/04/APPGReport2017-270217.pdf.

Example 1: making a conditional threat online

Davina decides to speak out to a local newspaper about the gender pay divide at her workplace. Davina receives a message on her Facebook timeline that evening from Jon, a former colleague of hers, which reads "You're a liar, I know you walk home and I could wait outside Widgets-R-Us and rape you. But I'm a nice guy so I won't. You're so ugly I couldn't even be bothered to rape you."

Analysis:

7.94 This is not an offence under section 16 of the OAPA 1861 as there is no threat to kill.

7.95 The conditionality in the threat, and the need to prove immediacy, would make it difficult to prosecute as an assault.[80]

7.96 As we have discussed above at paragraph 7.62, a prosecution under section 5 of the POA 1986 (displaying threatening or abusive writing within the sight of a person likely to be caused harassment, alarm or distress) is unlikely to be available in relation to online communications.

7.97 The other possible charges here are for the offences in section 1 of the MCA of the 1988 and section 127 of the CA 2003. On the latter, a message of a menacing character is sent over a public electronic communications network, and is at least likely to create fear or apprehension in Davina. Jon intended it to be of a menacing character, or was aware or would have recognised the risk that it would have created fear and apprehension in Davina.[81] In this scenario, it is likely that the more serious charge under section 1 of the MCA 1998 could also succeed, as the posting on Davina's timeline could be considered sending "to" her, and this was a threat which was clearly sent with intent to cause anxiety or distress.

80 See *Tuberville v Savage* (1669) 1 Mod 3.

81 *Chambers v DPP* [2012] EWHC 2157; [2013] 1 WLR 1833 at [38].

Example 2: overlapping offences

Lucas and Berat work together but have never seen eye to eye. Eventually, Berat decides to leave, but makes sure that he makes his feelings about Lucas known to many of their colleagues as he goes.

Lucas is furious about this and sends two emails to Berat's new work email address the following week. The first states:

> You're a useless pathetic individual. Did you think I wouldn't hear about all the lies you've been spreading? Everyone here hates you. You're rubbish at your job and just a massive loser really. Go fuck yourself you piece of shit.

The next day he sends another email:

> So I hear you tried to blame me for all your fuck ups?! Seems I will have to tell your new job all the terrible things about you. Enjoy your unemployment!

Analysis:

7.98 This example illustrates the range of offences that a prosecutor might have available should they wish prosecute charges against Lucas.

7.99 The emails could amount to an offence contrary to section 1 of the MCA 1988 on the basis that it contains a "threat"[82] ("Seems I will have to tell your new job all the terrible things about you"). It would be necessary to demonstrate that Lucas had the requisite mens rea; that one of his purposes was to cause Berat distress or anxiety.

7.100 They could also amount to an offence under section 4A of the POA 1986 if the prosecutor could demonstrate that Lucas intended to cause Berat harassment, alarm or distress and Berat in fact experienced harassment, alarm or distress as a result of the emails.

7.101 Finally, as multiple communications were sent, a charge of harassment contrary to section 2 of the PHA 1997 might be available if the prosecutor could demonstrate that the two emails amounted to a "course of conduct".

7.102 A communication offence is probably the most likely outcome in this case given that as conduct crimes, they are easier to demonstrate than the POA 1986 and PHA 1997 charges.

7.103 Interestingly, had Lucas made these statements in person, rather than online, it is rather unlikely that any prosecution (for example under the POA 1986) would follow. This example therefore also raises one of the overarching issues we have noted in this Report; that there are variety of contexts where online communication might be pursued

[82] Malicious Communications Act 1988, s 1(1)(a)(ii).

as a criminal offence in circumstances where equivalent offline communication would not.

CONCLUSION

7.104 None of the specific threats offences are a perfect fit with threatening behaviour online. All criminalise a certain amount of such behaviour, but have elements which do not match the characteristics of online communication.

7.105 The fault element of the threat to kill offence under section 16 of the OAPA 1861 – that the defendant must intend the victim to fear that the threat will be carried out – presents a high threshold for a prosecutor to reach. Arguably, however, this is entirely appropriate on or off line, and preserves the special character of what is a very serious offence. The uncertainty over what it means to make a threat to another may create arbitrary distinctions online, and may force prosecutions for lesser offences when the particular conduct warrants the more serious charge.

7.106 In the case of common assault, the requirement of immediacy may make it unsuitable for prosecution of many threats made online, and conditionality makes it too easy for the sorts of threatening language routinely used online to escape liability.

7.107 The public order offences were not designed for online offences and applying them online in their current forms presents some challenges. As we have seen they cannot be committed if perpetrator and victim are in a "dwelling". The section 4 of the POA 1986 offence (causing fear or provoking violence) requires that the threat be directed "towards another". Section 4A of the POA 1986 requires both that harassment, alarm or distress has actually been caused, and that the defendant intended it. As we note at paragraph 7.62 above, it is unclear whether section 5 of the POA 1986 can be applied online.

7.108 This overview also tends to support Alldridge's view that threat offences are complex and inconsistent, without clear conceptual underpinnings. They were drafted with quite specific, real world, conduct in mind, and therefore fit poorly with similar conduct when it occurs in cyberspace.

7.109 However, in the majority of cases the communication offences under the MCA 1988 and the CA 2003 will allow prosecution. As we outline in other parts of this Report, these offences have their own problems, and we have recommended that wider reform be considered.

Chapter 8: Harassment and stalking

INTRODUCTION

8.1 Harassment and stalking are concepts which are widely used and discussed in everyday life but have proved difficult to define for the purposes of the criminal law.[1]

8.2 Various forms of "harassment" may amount to a criminal offence in England and Wales, while separate "stalking" offences have been created which apply in relation to particular forms of harassment associated with specific kinds of "stalking" behaviour.

8.3 There are also definitions of harassment in other legal contexts, such as anti-discrimination law and employment law.[2]

8.4 Criminal harassment and stalking behaviours are not a new phenomenon, but the incredible connectivity of the online environment – while positive in many ways – also facilitates new means of harassment and stalking.[3]

8.5 For example, the creation of online dating apps – particularly those that make use of the users' geographic location – can expose users to people who might not otherwise have had such ready access to them. More broadly, widely used social networking, blogging and messaging tools provide harassers and stalkers with instantaneous, 24-hour access to their targets. Online gaming is another forum in which players are often subjected to harassment and abuse.[4]

8.6 Another important aspect of the problem is that women and girls are disproportionately affected by harassment and stalking. The Crime Survey for England and Wales indicates that women are twice as likely to be victims of this behaviour than men.[5] The prevalence of sexual harassment of women and girls, including online sexual harassment, was recently highlighted by Women and Equalities Committee of the

---

1 E Finch, "Stalking the perfect stalking law: an evaluation of the efficacy of the Protection from Harassment Act 1997" [2002] *Criminal Law Review* 702.

2 See Equality Act 2010, s 26.

3 J Clough, *Principles of Cybercrime* (2nd ed, 2015) p 417.

4 This was highlighted most prominently through the 2014 GamerGate controversy, which involved coordinated harassment of women in gaming. See B Stuart, *GamerGate: the misogynist movement blighting the video games industry* (24 October 2014), available at https://www.telegraph.co.uk/culture/culturenews/11180510/gamergate-misogynist-felicia-day-zoe-quinn-brianna-wu.html.

See, also more generally Ditch the Label, *In Game Abuse* (2017), available at https://www.ditchthelabel.org/research-papers/ingame-abuse/.

5 Office for National Statistics, *Domestic abuse, sexual assault and stalking* (9 February 2017), available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/compendium/focusonviolentcrimeandsexualoffences/yearendingmarch2016/domesticabusesexualassaultandstalking.

House of Commons of the House of Commons in its report into *Sexual harassment of women and girls in public places*.[6]

8.7 There is no distinct criminal offence of "online harassment" or stalking conduct committed online, sometimes referred to as "cyberstalking", but online behaviour may form the entirety of the conduct for the purposes of a more general harassment offence, or be part of a broader course of conduct that involves other elements such as verbal or physical contact.[7]

8.8 "Cyberbullying" is another, related concept which is often discussed in this context. It is typically associated with younger people, but may occur in other contexts such as employment.[8] There is no specific offence of "bullying" or "cyberbullying", and in this Report we consider it as a subset of the behaviours that might constitute stalking and harassment.

8.9 Research suggests that the prevalence of online harassment is high,[9] and stalking by a person unknown to the victim is more common online than offline.[10]

8.10 The use of technology such as malicious software can allow perpetrators to monitor all aspects of a victim's behaviour.[11] For example, smartphone apps that can track the movement and actions of a user have been developed, and used on unsuspecting victims.

8.11 Consistently with other forms of online abuse, and as we outline in greater detail in Chapter 2, harassment online is influenced by the disinhibition and lack of social cues in cyberspace, and the apparent anonymity/lack of monitoring.[12] This can make harassment and stalking conduct more intense than it otherwise might be.

8.12 The online world can vastly increase the audience and harm to a victim that can occur online. This includes harassing conduct such as "flaming" a victim by attacking them in

---

6 Sexual harassment of women girls in public places, Report of the Women and Equalities Committee of the House of Commons (October 2018) HC 701.

7 T Holt, A Bossler and K Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2nd ed, 2018) p 351. For a case example see *R v Cordle* [2016] EWCA Crim 1793; [2017] 1 Cr App R (S) 36, where the conduct involved a combination of emails, text messages and telephone calls.

8 J Clough, *Principles of Cybercrime* (2nd ed, 2015) p 420.

9 For example, a 2014 Pew Research Center study found that 40% of internet users have personally experienced some form of online harassment: Pew Research Center, *Online Harassment* (October 2014), available at http://assets.pewresearch.org/wp-content/uploads/sites/14/2014/10/PI_OnlineHarassment_72815.pdf.

10 See National Centre for Cyberstalking Research, *Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey* (2011), available at https://www.beds.ac.uk/__data/assets/pdf_file/0011/577721/ECHO_Pilot_Final.pdf.

11 T Holt, A Bossler and K Seigfried-Spellar, "Cybercrime and Digital Forensic: An Introduction" (2nd ed, 2018) p 350.

12 See BC Jones, "The Online/Offline Cognitive Divide: Implications for Law" 13(1) *Scripted* 83.

a public forum,[13] or "outing" a victim, by publishing private information that the person did not want to make public, causing them embarrassment or distress.[14]

8.13 Typical forms of cyberstalking include:

(1) repeated unsolicited communication using electronic means, for example social media, instant messaging applications, and email;

(2) impersonation of the victim, for example by creating false profiles on dating applications;

(3) publication of false information about the victim;

(4) unauthorised access to the personal information of the victim; and

(5) covert surveillance of the victim, including through "trojan" software.[15]

8.14 The impact on victims of cyberstalking and online harassment can be profound. A 2011 study by the National Centre for Cyberstalking Research identified that many victims experience post-traumatic stress disorder, with respondents to the survey identifying loss or change of employment, relationship breakdown and personal isolation amongst the effects.[16]

8.15 In this Chapter we consider specific offences of harassment and stalking that exist in England and Wales, as well as other offences that relate to harassing or stalking behaviour or might be committed in such a context.

8.16 We also outline in brief the civil remedies, such as protective orders and civil compensation, that might be available to a victim of harassment or stalking behaviour.

8.17 We conclude by providing examples of some of the particular challenges that arise in the context of pursuing criminal sanctions for harassment and stalking behaviour that is committed online.

THE LAW GOVERNING HARASSMENT AND STALKING

8.18 The law governing the offences of harassment and stalking and related remedies is primarily found in the Protection from Harassment Act 1997 ("PHA 1997"). This Act was

---

13 "Flaming" is generally understood, in the context of internet communications, as an abusive and insulting conversation between people online. It can often involve two or more individuals targeting another.

14 A Gillespie, *Cybercrime: Key Issues and Debates* (2016) p 258.

15 N MacEwan, "The New Stalking Offences in English Law: Will they Provide Effective Protection from Cyberstalking?" [2012] 10 *Criminal Law Review* 767, pp 773 to 774. "Trojan" software refers to software that is misleading as to its real purpose or use.

16 National Centre for Cyberstalking Research, *Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey* (2011) p 31, available at https://www.beds.ac.uk/__data/assets/pdf_file/0011/577721/ECHO_Pilot_Final.pdf.

introduced to clarify the law in relation to stalking and harassment, and provide more clear and certain remedies.[17]

8.19 In particular, prior to the PHA 1997, there was limited protection for victims who were upset and frightened by a series of disturbing incidents, each one of which, viewed individually, fell short of criminal conduct.[18]

8.20 Various revisions were made in the early 2000s to cater for group and collective harassment,[19] and the PHA 1997 was significantly amended in 2012, when the offences of stalking, and of stalking involving fear of violence or serious alarm or distress, were introduced.[20]

8.21 Updated Sentencing Council Guidelines for "Intimidatory Offences", which largely relate to PHA 1997 offences, came into force in October this year.[21]

8.22 A separate offence of harassment at home was also introduced by the Serious Organised Crime and Police Act 2005.[22]

8.23 Prior to the introduction of the PHA 1997, some forms of harassment could be pursued as an offence under section 4A and 5 of the Public Order Act 1986 ("POA 1986"),[23] or under the Offences Against the Person Act 1861.[24] These laws remain in force and are prosecuted in certain contexts, although PHA 1997 charges will generally be preferred where a "course of conduct" can be demonstrated.

8.24 Since late 2015, stalking or harassment that occurs in the context of an intimate relationship can also be pursued as an offence of coercive and controlling behaviour under section 76 of the Serious Crime Act 2015. This offence was introduced to address cases of domestic abuse where a victim is subject to a pattern of abusive behaviour in the context of an intimate relationship. As with stalking and harassment, the offence renders conduct criminal when performed as a course of action in circumstances where each incidence might not necessarily amount to an offence in its own right.

8.25 Harassment or stalking that involves sending some form of communication might also be pursued as an offence of improper use of a public electronic communications network under section 127 of the Communications Act 2003 ("CA 2003"), or a malicious

---

17 *Hansard* (HL), 24 January 1997, vol 577, col 917 (Lord Mackay of Clashfern, then Lord Chancellor).

18 J Harris, *An evaluation of the use and effectiveness of the Protection from Harassment Act 1997* (Home Office Research Study 203, 2000).

19 See further paragraphs 8.39 to 8.52 below.

20 Protection of Freedoms Act 2012, s 111.

21 Sentencing Council, *Intimidatory Offences: Definitive Guideline* (effective 1 October 2018), available at https://www.sentencingcouncil.org.uk/wp-content/uploads/Intimidatory-Offences-Guideline_WEB.pdf.

22 Serious Organised Crime and Police Act 2005, s 126. This provision created the offence in section 42A of the Criminal Justice and Police Act 2001.

23 The offences are intentional harassment, alarm or distress under section 4a, and harassment, alarm or distress under section 5 of Public Order Act 1986.

24 For example, in the case of *R v Ireland* [1998] AC 147, harassing phone calls that led to psychiatric injury were found to amount to offences under sections 20 and 47 of the Offences Against the Person Act 1861.

communication under section 1 of the Malicious Communications Act 1988 ("MCA 1988"). We discuss these offences in greater detail in Chapter 4.

8.26 Below we consider the harassment and stalking offences and remedies in more detail.

Offence of harassment under the PHA 1997

8.27 The offence of harassment is a summary only offence that carries a maximum penalty of six months' imprisonment or a fine.[25]

8.28 It was originally conceived as an offence committed by one person against another, but has evolved to include harassment of groups, which we detail further below.

What is meant by "harassment"?

8.29 The definition of the offence of harassment of another in the PHA 1997 is: "a course of conduct, which amounts to harassment of another, and which [the defendant] knows or ought to know amounts to harassment of the other".[26]

8.30 Section 7 of the Act states that harassing a person includes "alarming the person or causing the person distress".[27]

8.31 "Conduct" that may amount to harassment includes speech.[28]

8.32 While the victim of harassment must be a natural person,[29] the perpetrator may be a corporate entity.[30]

8.33 The term harassment was given further definition by the Court of Appeal in *Thomas v News Group Newspapers*:

> The Act does not attempt to define the type of conduct that is capable of constituting harassment. "Harassment" is, however, a word which has a meaning which is generally understood. It describes conduct targeted at an individual which is calculated to produce the consequences described in section 7 and which is oppressive and unreasonable. The practice of stalking is a prime example of such conduct.[31]

---

25 Protection from Harassment Act 1997, s 2(2).

26 Protection from Harassment Act 1997, s 1(1).

27 Protection from Harassment Act 1997, s 7(2).

28 Protection from Harassment Act 1997, s 7(4).

29 Protection from Harassment Act 1997, s 7(5).

30 *Kosar v Bank of Scotland* [2011] EWHC 1050 (Admin).

31 *Thomas v News Group Newspapers Ltd*; [2001] EWCA Civ 1233; [2002] Entertainment and Media Law Reports 4 at [30]. This definition was further endorsed by the Supreme Court in *Hayes v Willoughby* [2013] UKSC 17; [2013] 1 WLR 935.

8.34 To warrant the imposition of criminal liability, the conduct must cross "the boundary between conduct which is unattractive, even unreasonable, and conduct which is oppressive and unacceptable."[32]

8.35 The fault element of the offence is that the defendant "knows or ought to know" that their conduct amounts to harassment of the other person. Whether a defendant "ought to know" is assessed by reference to whether a reasonable person in possession of the same information would think the course of conduct amounted to harassment.[33] It is a purely objective test and does not take into account the circumstances as the defendant perceived them to be.[34]

8.36 For example, if a defendant subjectively perceives that sending a series of loving emails and digital photos to another is welcome and appreciated, this does not excuse the harassing conduct if a reasonable person in the defendant's position would think that this conduct actually amounted to harassment.

8.37 The Court of Appeal has rejected attempts to argue that a different standard should be applied for perpetrators suffering from mental illness.[35] In particular, the Court has noted that "the conduct at which the Act is aimed, and from which it seeks to provide protection, is particularly likely to be conduct pursued by those of obsessive or otherwise unusual psychological make-up and very frequently by those suffering from an identifiable mental illness".[36] The Court further found that given that the overriding purpose of the legislation is to protect victims, to set a different standard in the Act for defendants with mental illness would "remove from its protection a very large number of victims and indeed run the risk of significantly thwarting the purpose of the Act".[37]

8.38 To commit the offence, there must be a "course of conduct" amounting to harassment. In other words, there must be more than one instance of conduct on the part of the defendant in relation to the victim.[38] However, there need only be one result from the cumulative effect of the defendant's course of conduct, namely the harassment of the victim.[39] This means that conduct that may not initially have been experienced as harassment by the victim (for example, liking or tagging content online) may still be

---

32 *Majrowski v Guy's and St. Thomas' NHS Trust* [2006] UKHL 34; [2007] 1 AC 224 at [30]. See also *R v Tan* [2017] EWCA Crim 493 at [18], where the Court approved of this test, although noted that a judge need not actually use the words "oppressive and unacceptable" (which do not appear in the Protection from Harassment Act 1997) in describing the conduct to a jury; the judge could, as in this case, instead provide examples of such conduct for the jury.

33 Protection from Harassment Act 1997, s 1(2).

34 *R v Colohan* [2001] EWCA Crim 1251; [2001] *Criminal Law Review* 845.

35 *R v Colohan* [2001] EWCA Crim 1251; [2001] *Criminal Law Review* 845. However, this does not preclude the defence of insanity being available in circumstances where a person does not know the nature and quality of their act, or does not know that what they are doing is wrong, in the sense of the conduct being contrary to law. See *Loake v DPP* [2017] EWHC 2855 (Admin); [2018] 2 WLR 1159.

36 *R v Colohan* [2001] EWCA Crim 1251; [2001] *Criminal Law Review* 845 at [18].

37 *R v Colohan* [2001] EWCA Crim 1251; [2001] *Criminal Law Review* 845 at [19].

38 Protection from Harassment Act 1997, s 7(3)(a).

39 *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233; [2002] Entertainment and Media Law Reports 4 at [29] to [30].

considered part of a course of conduct if – in combination with other behaviour by the defendant (for example, an unwanted phone call or attendance at the victim's residence) – the victim later experiences this as part of an ongoing course of harassing conduct on the part of the defendant.

Collective harassment

8.39 A person who commits a course of conduct amounting to harassment with the requisite knowledge or intention is liable as a principal offender. However, a person may also be liable as a secondary party where he assisted or encouraged the principal offender to commit the offence. In addition to the act or acts which assist or encourage the offender, the secondary party must know any existing facts necessary for their conduct to be criminal.[40]

8.40 Where a defendant carries out a course of conduct which amounts to harassment of a victim as described above, it would be possible for another person to be liable as secondary party to that conduct.[41] For example, "D1" writes and hand-delivers a large volume of abusive and distressing letters to his local MP over the course of a week to protest about a local planning decision. Therefore, D1 pursues a course of conduct which he knows or ought to know amounts to harassment. "D2" is present when D1 composes some of the letters and knows of their content. With this knowledge, D2 drives D1 to the victim's home on a number of occasions so D1 can deliver them to the victim. In these circumstances, D2 may be liable as a secondary party for assisting D1 to commit the offence of harassment.

8.41 In 2001, section 7(3A) of the PHA 1997 was introduced[42] to counter group harassment. The provision draws on accessory liability principles, and provides:

> A person's conduct on any occasion shall be taken, if aided, abetted, counselled or procured by another–
>
> (a) to be conduct on that occasion of the other (as well as conduct of the person whose conduct it is); and
>
> (b) to be conduct in relation to which the other's knowledge and purpose, and what he ought to have known, are the same as they were in relation to what was contemplated or reasonably foreseeable at the time of the aiding, abetting, counselling or procuring.

8.42 The broader context surrounding this, and other reforms made to harassment laws in the Criminal Justice and Police Act 2001,[43] included concern about the conduct of

---

40 *R v Jogee* [2016] 2 WLR 681.

41 Magistrates' Court Act 1980, s 44. See also Accessories and Abettors Act 1861, s 8 in respect of indictable offences.

42 This provision was introduced by section 44 of the Criminal Justice and Police Act 2001.

43 eg, the introduction of the offence of harassment at home, contrary to section 42A of the Criminal Justice and Police Act 2001.

animal rights protesters in respect of pharmaceutical research companies and their employees.[44] The explanatory note to the relevant provision states:

> Section 44 amends the Protection from Harassment Act 1997 to make it clear that the legal sanctions that apply to a campaign of harassment by an individual against another also apply to a campaign of collective harassment by two or more people. It is an offence under section 2 of that Act to pursue a course of conduct against someone which amounts to harassment and which the person responsible knows or ought to have known amounts to harassment…
>
> Subsection (1) amends section 7 of the 1997 Act, which provides for the interpretation of 'conduct' and 'course of conduct' in sections 1 to 5, by inserting a new subsection (3A). Paragraph (a) provides that conduct by one person shall be taken, at the time it occurs, also to be conduct by another if it is aided, abetted, counselled or procured by that other person.
>
> Paragraph (b) provides that the knowledge and purpose of those who aid, abet, counsel or procure such conduct relate to what was contemplated or reasonably foreseeable at the time of the aiding, abetting, counselling or procuring. This enables knowledge and purpose to be viewed in relation to what was planned or should have been expected at the time of planning.

8.43 The drafting of the provision is complex, however, its effect is to:

(1) specify that a campaign of collective harassment by two or more people can amount to a "course of conduct"; and

(2) confirm that one person can pursue a course of conduct by committing one act personally and arranging for another person to commit another act.

8.44 So, for example, if "D1" sent a single harassing email to a victim, and then helped another three people, "D2", "D3" and "D4" to draft harassing emails which each of them individually sent, D1 could be held liable for harassment by virtue of section 7(3A). This deems the conduct of the other three individuals to form part of D1's conduct, because the defendant has aided, abetted, counselled or procured it.

8.45 Further, when section 7(3A) of the PHA 1997 is combined with the 2005 amendment criminalising harassment against a group[45] (see paragraphs 8.49 to 8.52 below), it is possible that charges could be pursued against a defendant who organises a campaign of harassment against a group involving multiple victims and multiple harassers. This could work as follows:

---

[44] See Home Office, *Animal Rights Extremism: Government Strategy* (Consultation Document, March 2001), available at http://www.fraw.org.uk/library/direct_action/home_office_2001.pdf; and Home Office, *Animal Welfare – Human rights: protection people from animal rights extremists* (July 2004), available at http://webarchive.nationalarchives.gov.uk/20081023120145/http:/police.homeoffice.gov.uk/publications/operational-policing/humanrights.pdf?view=Binary.

[45] Protection from Harassment Act 1997, s 1(1A), inserted by the Serious Organised Crime and Police Act 2005, s 125(2)(a).

(1) The defendant sends a harassing tweet to a member of an animal rights group seeking to intimidate them so they do not engage in a lawful protest;

(2) The defendant aids, abets, counsels or procures ten other individuals to send harassing tweets to other members of the animal rights group, also seeking to intimidate them so they do not engage in a lawful protest. Each of the members of the group does so;

(3) The defendant has therefore arguably committed a section 2 harassment offence as he or she has committed a course of conduct by participating in and aiding, abetting, counselling or procuring (section 7(3A) of the PHA 1997) the harassment of a group (section 1(1A) of the PHA 1997).

8.46 We are not aware of any harassment prosecutions being constructed in this way, and indeed there has been very little reported criminal case law in relation to collective harassment under section 7(3A). It was considered in the context of a civil harassment claim in the case of *Hourani v Thomson*.[46] In this case, the High Court considered liability for a "campaign" of harassment against Mr Hourani orchestrated by several defendants. One of the defendants argued that they engaged in only one instance of conduct, and therefore had not engaged in harassment. Mr Justice Warby rejected the argument that only one act had occurred, but further ruled that:

> [the defendant's] own role in bringing about the [protest event against the claimant] involved conduct on more than one occasion; and even if that were not so, it is plain that what [other co-defendants] did to bring about the online publications involved conduct on multiple occasions, which is attributable to [the defendant] pursuant to section 7(3A), because he aided and abetted that conduct.[47]

8.47 While section 7(3A) makes it technically possible to pursue collective harassment, there is little evidence that the PHA 1997 is being used for this purpose. The complex and somewhat unclear manner in which the provision is drafted is one possible cause of this. Further, given harassment is a summary offence, the construction of charges based on intricate notions of secondary liability would likely be viewed by prosecutors as disproportionate in the majority of cases.

8.48 However, as we outlined in Chapter 3, group harassment is a very real problem online with the potential to ruin victims' lives. Later in this Chapter, we consider whether there is scope for the law to target group conduct in a more clear and direct manner.

Harassment of two or more persons

8.49 In 2005, a further offence of harassment of two or more persons was enacted.[48] This offence is intended to protect groups – for example a family or particular religious or

---

46 [2017] EWHC 432 (QB).

47 *Hourani v Thomson* [2017] EWHC 432 (QB) at [136].

48 Protection from Harassment Act 1997, s 1(1A).

ethnic groups – from harassment. The offending conduct must be committed by an individual person,[49] and has the following elements:

(1) a course of conduct;

(2) which involves harassment of two or more persons; and

(3) which the defendant knows or ought to know involves harassment of those persons;

(4) by which the defendant intends to persuade any person:

(a) not to do something that they are entitled or required to do; or

(b) to do something that they are not under any obligation to do.[50]

8.50 This form of the offence has an additional fault element, namely an intention to persuade any person to do or not do something.

8.51 Whereas a "course of conduct" for the purposes of harassment against one person requires more than one occasion of conduct in relation to that victim, harassment of two or more persons requires at least one occasion of conduct in relation to each of those persons.[51]

8.52 For example, if an individual were to send separate single WhatsApp messages to multiple members of their ex-partner's family, seeking to persuade the family members not to attend their ex's engagement party, this could amount to harassment of two or more persons under the PHA 1997.

What is meant by a "course of conduct"?

8.53 To amount to a course of conduct for the purposes of harassment offences, there must be a sequence of connected events, which should not be too distantly related in time.[52] It is not necessary that each individual event amounts to a crime in its own right,[53] and the complainant may find out about the conduct from a third party.[54] However, the fewer the incidents, the more serious each is likely to have to be to amount to a course of harassment.[55]

---

49 Protection from Harassment Act 1997, s 7(5).

50 Protection from Harassment Act 1997, s 1(1A).

51 Protection from Harassment Act 1997, s 7(3).

52 *Lau v DPP* [2000] *Criminal Law Review* 580.

53 *Jones v DPP* [2010] EWHC 523 (Admin); [2011] 1 WLR 833 at [27].

54 See *Kellett v DPP* [2001] EWHC 107 (Admin).

55 *Jones v DPP* [2010] EWHC 523 (Admin); [2011] 1 WLR 833 at [35].

8.54 In *R v Patel*,[56] a case involving evidence of two or three incidents of domestic abuse of a woman by her husband, the Court of Appeal emphasised the need to demonstrate a nexus between events for them to amount to a course of conduct:

> It is not just a matter of counting the incidents and saying, 'We have two, that is enough.' It is necessary for the jury to be given some guidance so that they address the question of whether the incidents give rise to a nexus sufficient for there to be a course of conduct… the issue is whether or not the incidents, however many there may be, can properly be said to be so connected in type and in context as to justify the conclusion that they can amount to a course of conduct.[57]

8.55 In some instances, conduct of the defendant interspersed between an otherwise harassing course of conduct may mean that no crime is committed. In the case of *R v Curtis*,[58] the Court of Appeal considered whether six violent or threatening incidents that occurred in the course of a nine month relationship amounted to the PHA 1997 offence of putting a person in fear of violence.[59] While finding that "the jury would have been entitled… to conclude that, over the course of the relationship, the defendant's conduct was deplorable" and the "the incidents were far from trivial", the outbursts of aggression were interspersed "with considerable periods of affectionate life". The Court therefore considered the conduct did not amount to a "course of conduct" for the purposes of the offence.[60]

8.56 The offence of coercive and "coercive and controlling behaviour in an intimate or family relationship" (discussed further below at paragraphs 8.97 to 8.107 below) may have been easier to demonstrate in a case such as *Curtis*, but had not been enacted at the relevant time.

What conduct can "amount to harassment"?

8.57 While harassment is loosely defined in the PHA 1997, courts have determined that there is a line between conduct that is unattractive and unreasonable (which is not criminal), and conduct which amounts to "torment" of the victim and is "of an order which would sustain criminal liability".[61]

8.58 In *Dowson v Northumbria Police*, the High Court considered a civil claim for harassment by six police officers relating to the conduct of a Chief Constable. Mr Justice Simon found that some of the conduct complained of, in particular repeated critical statements about one of the complainants in front of others, was "insensitive, belittling and overbearing". However, Mr Justice Simon found that:

> it was not conduct which was calculated to cause distress and, although it was unacceptable, it was not oppressive in the sense described in the cases. It was not a

---

56 [2004] EWCA Crim 3284; [2005] 1 Cr App R 27.

57 [2004] EWCA Crim 3284; [2005] 1 Cr App R 27 at [40].

58 [2010] EWCA Crim 123; [2010] 1 WLR 2770.

59 Protection from Harassment Act 1997, s 4.

60 [2010] EWCA Crim 123; [2010] 1 WLR 2770 at [32].

61 *Dowson v Northumbria Police* [2010] EWHC 2612 (QB) at [142].

tormenting by constant interference or intimidation. Rather it was a curt and dismissive attitude which was likely to have the effect, even if unintended, of undermining both [the complainant's] own self-confidence and the esteem in which he was held by others.[62]

8.59 In *Ferguson v British Gas Trading Ltd*, another civil claim for damages, the Court of Appeal found that a series of unwarranted computer-generated bills and letters demanding payment for sums not actually owed was at least capable of being found to be harassment, and therefore the claim should be allowed to proceed to trial.[63]

8.60 To amount to harassment, there must be a minimum degree of alarm or distress experienced by the defendant.[64] However, in *R v N*,[65] the Court of Appeal emphasised that causing alarm or distress to the victim is not on its own determinative of harassment, and the conduct must also be "oppressive".[66]

8.61 Examples of conduct that courts have held to constitute harassment include:

(1) surveillance in an attempt to prove that an individual was committing benefit fraud;[67]

(2) harassment by posting and threatening to post private and confidential information about the claimant on the internet;[68]

(3) harassment by publication of a series of newspaper articles;[69]

(4) threatening communications via the internet;[70]

(5) letters repeatedly attacking the professional integrity of a solicitor;[71] and

(6) circumstances where the victim has initiated contact with the defendant as part of her employment duties and received verbal abuse in response during telephone calls.[72]

Defences

---

62 *Dowson v Northumbria Police* [2010] EWHC 2612 (QB) at [278].

63 *Ferguson v British Gas Trading Ltd* [2009] EWCA Civ 46; [2010] 1 WLR 785.

64 *DPP v Ramsdale* [2001] EWHC Admin 106; *Independent*, March 19, 2001.

65 [2016] EWCA Crim 92; [2016] 2 Cr App R 10.

66 [2016] EWCA Crim 92; [2016] 2 Cr App R 10 at [32].

67 *Howlett v Holding* [2006] EWHC 41 (QB); (2006) 150 Solicitors Journal Law Brief 161.

68 *WXY v Gewanter* [2012] EWHC 496 (QB).

69 *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233; [2002] Entertainment and Media Law Reports 4.

70 *Neocleous v Jones* [2011] EWHC 3459 (QB); [2011] Info TLR 39.

71 *Iqbal v Dean Manson Solicitors* [2011] EWCA Civ 123; [2011] CP Rep 26.

72 *James v Crown Prosecution Service* [2009] EWHC 2925 (Admin); [2010] *Criminal Law Review* 580.

8.62 Certain contexts are excluded from the offence, notably conduct intended for the purpose of preventing or detecting crime, conduct pursued in accordance with a legal requirement or conduct that was reasonable in the particular circumstances of the case.[73]

8.63 The defence of "preventing or detecting a crime" was considered in detail in *Hayes v Willoughby*.[74] This case involved a situation where a former employee sent numerous letters to law enforcement agencies alleging his former employer was involved in fraud, embezzlement and tax evasion. The allegations were found to have no factual basis but the defendant persisted. At trial, the employee was found to have established the defence of "preventing or detecting a crime", but this finding was overturned at the Court of Appeal.

8.64 The case then progressed to the Supreme Court. In dismissing the employee's appeal, Lord Sumption (with whom the majority agreed) noted that although the defence was "no doubt drafted mainly with an eye to the prevention or detection of crime by public authorities" it "applies equally to private persons who take it upon themselves to enforce the criminal law".[75] However, His Lordship went on to state that:

> It cannot be the case that the mere existence of a belief, however absurd, in the mind of the harasser that he is detecting or preventing a possibly non-existent crime, will justify him in persisting in a course of conduct which the law characterises as oppressive. Some control mechanism is required, even if it falls well short of requiring the alleged harasser to prove that his alleged purpose was objectively reasonable.[76]

8.65 While an objective standard of reasonableness in the belief was not part of the test, Lord Sumption found that as a minimum, the person seeking to rely on the defence "must have thought rationally about the material suggesting the possibility of criminality and formed the view that the conduct said to constitute harassment was appropriate for the purpose of preventing or detecting it".[77]

Offence of stalking

8.66 Conduct amounting to "stalking" has always fallen within the offence of harassment,[78] but it was introduced as a specific offence by the Protection of Freedoms Act 2012.[79] It has a maximum penalty of six months' imprisonment and/or a fine.[80]

---

73 Protection from Harassment Act 1997, s 1(3). It is for the prosecution to demonstrate that these defences do not apply – see S Leake (ed), *Archbold Magistrates' Courts Criminal Practice 2019* (2018), paras 13 to 93.

74 [2013] UKSC 17; [2013] 1 WLR 935.

75 *Hayes v Willoughby* [2013] UKSC 17; [2013] 1 WLR 935 at [13].

76 *Hayes v Willoughby* [2013] UKSC 17; [2013] 1 WLR 935 at [13].

77 *Hayes v Willoughby* [2013] UKSC 17; [2013] 1 WLR 935 at [15].

78 *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233; [2002] Entertainment and Media Law Reports 4 at [30].

79 Protection of Freedoms Act 2012, s 111.

80 Protection from Harassment Act 1997, ss 2A(4) and (5).

8.67 An offence of stalking is committed where:

(1) the person has engaged in a course of conduct that amounts to harassment;

(2) the acts or omissions involved are ones associated with stalking; and

(3) the person whose course of conduct it is knows or ought to know that the course of conduct amounts to harassment of the other person.[81]

8.68 The offence of stalking has the same fault element as the offence of harassment, but the prosecution must prove to the criminal standard that the actions of the defendant amount to stalking.

8.69 There is no additional overarching definition of stalking, but the PHA 1997 includes a non-exhaustive list of acts and omissions which may be "associated" with stalking:[82]

(1) following a person;

(2) contacting, or attempting to contact, a person by any means;

(3) publishing any statement or other material

(a) relating or purporting to relate to a person; or

(b) purporting to originate from a person;

(4) monitoring the use by a person of the internet, email or any other form of electronic communication;

(5) loitering in any place (whether public or private);

(6) interfering with any property in the possession of a person;

(7) watching or spying on a person.

8.70 It is for the court to determine, in the light of all the evidence, whether stalking has taken place.

Fear of violence offences

8.71 The PHA 1997 also contains more serious offences of putting people in fear of violence, and stalking involving fear of violence or serious alarm or distress. These are either-way offences that since April 2017 have a maximum penalty of ten years' imprisonment on indictment.[83]

---

81 Protection from Harassment Act 1997, s 2A(2).

82 See the Protection from Harassment Act 1997, s 2A(3).

83 Protection from Harassment Act 1997, ss 4 and 4A. The previous maximum penalties were five years' imprisonment, but this was increased to 10 years by the Policing and Crime Act 2017, s 175(1).

Putting people in fear of violence – section 4 of the PHA 1997

8.72 The offence of putting people in fear of violence may be committed where a person causes another to fear, on at least two occasions, that violence will be used against them.[84]

8.73 A prosecution for this offence requires proof that harassment according to section 1 of the PHA 1997 has occurred, including that the behaviour was "oppressive and unreasonable".[85]

8.74 The fault element is that the defendant knows or ought to know that their course of conduct will cause the other to fear violence on each of those occasions. This is assessed according to the standard of the "reasonable person in possession of the same information" as the defendant.[86]

8.75 One possible way in which this offence might be committed is through threats being made by the defendant (which we consider in more detail in Chapter 7). However, it is not necessary that explicit threats are made, provided that it can be shown that the victim feared violence would be used against them.

Stalking involving fear of violence – section 4A(1)(b)(i) of the PHA 1997

8.76 This offence is similar to the section 4 offence referred to above, but has the additional requirement that the conduct amounts to stalking.[87]

8.77 The offence of stalking involving fear of violence may be committed where a person commits a course of conduct that amounts to stalking (as per the definition under section 2A of the PHA 1997), and the conduct causes the victim to fear on at least two occasions that violence will be used against them.

8.78 The fault element for this offence is that the defendant "knows or ought to know" that their conduct will cause the victim to fear that violence will be used against them on each occasion.[88]

Stalking involving serious alarm or distress – section 4A(1)(b)(ii) of the PHA 1997

8.79 Stalking involving serious alarm or distress (which may fall short of causing fear of violence) is another variant of the section 4A offence, and may be established where the stalking "causes another serious alarm or distress which has a substantial adverse effect on his or her usual day-to-day activities".[89]

---

84 Protection from Harassment Act 1997, s 4(1).

85 *R v Haque* [2011] EWCA Crim 1871; [2012] 1 Cr App R 5 at [69] to [70].

86 Protection from Harassment Act 1997, s 4(2).

87 Protection from Harassment Act 1997, s 4A(1)(a).

88 Protection from Harassment Act 1997, s 4A(1). This is again assessed according to the standard of the "reasonable person in possession of the same information" as the defendant: Protection from Harassment Act 1997, s 4A(2).

89 Protection from Harassment Act 1997, s 4A(1)(b)(ii).

8.80 The fault element of the offence is that the defendant knows or ought to know (by reference to the reasonable person in possession of the same information) that their course of conduct will cause the victim serious alarm or distress which has a substantial adverse effect on their usual day-to-day activities.[90]

8.81 The phrase "substantial adverse effect on ... usual day-to-day activities" is not further defined, but Home Office guidelines suggest that it might include:

- the victim changing their routes to work, work patterns, or employment;
- the victim arranging for friends or family to pick up children from school (to avoid contact with the stalker);
- the victim putting in place additional security measures in their home;
- the victim moving home;
- physical or mental ill-health;
- the deterioration in the victim's performance at work due to stress; and
- the victim stopping or changing the way they socialise.[91]

8.82 Defences are available where the conduct was intended for the purpose of preventing or detecting crime, was pursued in accordance with a legal requirement, or was reasonable to protect the defendant or another or to protect their property.[92]

Hate aggravated offending

8.83 Harassment and stalking that is proven to be motivated by or has involved a demonstration of hostility based on one of five protected characteristics: race, religion, sexual orientation, disability or transgender status will be subject to aggravated sentences under sections 145 and 146 of the Criminal Justice Act 2003. We discuss hate crime in more detail in Chapter 9, but we outline the key aspects below.

Racially or religiously aggravated offending

8.84 Harassment and stalking that is racially or religiously aggravated may also amount to an aggravated offence under section 32 of the Crime and Disorder Act 1998.

8.85 For example, in March 2018, the leader and deputy leader of "Britain First" were convicted of racially aggravated harassment (amongst other offences) following the

90 Protection from Harassment Act 1997, s 4A(3).

91 Home Office, "A change to the Protection from Harassment Act 1997: introduction of two new specific offences of stalking" (Circular 018/2012, 15 October 2012), available at http://www.homeoffice.gov.uk/about-us/corporate-publications-strategy/home-office-circulars/circulars-2012/018-2012/.

92 Protection from Harassment Act 1997, s 4A(4).

distribution of leaflets and the posting of online videos during a gang-rape trial. They were sentenced to 18 and 36 weeks' imprisonment respectively.[93]

8.86 The offence requires proof of the harassment offence as described above, and in addition proof of demonstrated hostility on grounds of race or religion or that the offence was motivated by such hostility.

8.87 In more detail, the conduct will be considered racially or religiously aggravated if the prosecution prove to the criminal standard that—

(1) at the time of committing the offence, or immediately before or after doing so, the offender demonstrates towards the victim of the offence hostility based on the victim's membership (or presumed membership) of a racial or religious group; or

(2) the offence is motivated (wholly or partly) by hostility towards members of a racial or religious group based on their membership of that group.[94]

8.88 A finding that the offender demonstrated racial or religious hostility in the stalking conduct does not require proof that they were motivated by racial or religious hostility.[95] For example, the offender may use racial or religious slurs because they know they will upset the victim, rather than because they actually harbour hostility towards the racial group.

8.89 A finding that the offence was motivated by racial or religious hostility requires evidence that the offender harboured such hostility, and at least one of their motivations (but not necessarily the primary motive) for the harassment was this hostility.[96]

8.90 It is necessary to prove that the hostility was based on the victim's membership (or presumed membership) of a racial or religious group. There can be particular challenges in proving this in the online environment. For example, where only a small amount of information is available from a victim's social media profile, a defendant may seek to argue that they were not aware of the victim's race or religion and did not presume that the person was a member of the relevant racial or religious group.

8.91 The effect of a finding of racial or religious aggravation is to increase the maximum penalty for harassment and stalking to up to two years (from six months), and the offence of stalking involving fear of violence or serious alarm or distress to 14 years (from 10 years).[97]

Other forms of hate crime: sexual orientation, disability or transgender status

8.92 There are no specific aggravated offences for harassment or stalking behaviour that demonstrates or is motivated by hostility based on sexual orientation, disability or

---

93 BBC, *Britain First leader and deputy leader jailed for hate crimes* (7 March 2018), available at https://www.bbc.co.uk/news/uk-england-43320121.

94 Crime and Disorder Act 1998, s 28(1).

95 *Jones v DPP* [2010] EWHC 523 (Admin); [2011] 1 WLR 833 at [17].

96 *DPP v McFarlane* [2002] EWHC 485 (Admin); *DPP v Howard* [2008] EWHC 608 (Admin).

97 Crime and Disorder Act 1998, s 32(3), (4).

transgender status. However, where the court is satisfied of such, the court must treat this as an aggravating factor in sentencing.[98] The same is also true for other racially or religiously aggravated offending that is not specified as an aggravated offence under the Crime and Disorder Act 1998.[99]

Protective orders and compensation for harassment

Restraining orders

8.93 On either conviction[100] or acquittal[101] of any criminal offence, the court may make a restraining order prohibiting the defendant from doing anything described in the order.

8.94 The orders are intended to be preventive and protective, not punitive, but breach of such an order carries a maximum penalty of up to five years' imprisonment.[102]

8.95 This can be a very important way of protecting victims from further harassment or stalking conduct.

Civil compensation

8.96 In addition to criminal offences, the PHA 1997 also created the tort of stalking and harassment, which allows a person to seek damages for (among other things) any anxiety caused by the harassment and any financial loss resulting from the harassment.[103] Such a civil claim requires a finding that the criminal offence of harassment has been committed, albeit that it need only be demonstrated to the civil standard of proof.[104]

Offence of coercive and controlling behaviour in an intimate or family relationship

8.97 The offence of coercive and controlling behaviour in an intimate or family relationship was introduced by the Serious Crime Act 2015.

8.98 The then Home Secretary Theresa May stated that it was intended to address domestic abuse involving "a pattern of non-violent controlling conduct, the cumulative impact of which can be no less traumatic for the victim".[105]

8.99 The repeated, non-violent nature of the conduct covered by the offence bears some similarity to the PHA 1997 offences, although it is better adapted to abuse within the context of ongoing relationships.

---

98 Criminal Justice Act 2003, s 146.

99 Crime and Disorder Act 1998, s 145.

100 Protection from Harassment Act 1997, s 5.

101 Protection from Harassment Act 1997, s 5A.

102 Protection from Harassment Act 1997, s 6.

103 Protection from Harassment Act 1997, s 3(2).

104 *Ferguson v British Gas Trading Ltd* [2009] EWCA Civ 46; [2010] 1 WLR 785.

105 *Hansard* (HC), 5 January 2015, vol 590, col 63 (The Rt Hon Theresa May MP).

8.100 The offence is committed where:

- the defendant repeatedly or continuously engages in behaviour towards another person, the victim, that is controlling or coercive; and
- at the time of the behaviour, the defendant and victim are personally connected; and
- the behaviour has a serious effect on the victim; and
- the defendant knows or ought to know that the behaviour will have a serious effect on the victim.[106]

8.101 "Serious effect" is further defined to mean either that the behaviour causes the person to fear, on at least two occasions, that violence will be used against them, or causes serious alarm or distress which has a substantial adverse effect on their usual day-to-day activities.[107]

8.102 The offence applies only where the victim and defendant are "personally connected", which means that they are in an intimate personal relationship (whether or not living together) or live together and are family members or have previously been in an intimate personal relationship.[108]

8.103 The requirement of personal connection means that it is less likely than harassment and stalking that the offending will be committed solely online, but it certainly could include an online element; for example, sending controlling messages or seeking to control the victim's online behaviour.

8.104 It is a defence if the defendant can show that, in engaging in the prohibited behaviour, the defendant believed that he or she was acting in the victim's best interests, and in all the circumstances the behaviour was reasonable.[109] However, this defence is not available in circumstances where the defendant has caused the victim to fear violence will be used against them.[110]

8.105 The defence has been criticised as potentially playing into societal preconceptions about what kind of behaviour is "reasonable" in a relationship, and creating a hierarchy of harm. In such a hierarchy, the concern is that while it is never acceptable to cause someone to fear that violence will be used against them, it could be found to be

---

106 Serious Crime Act 2015, s 76(1).

107 Serious Crime Act 2015, s 76(4).

108 Serious Crime Act 2015, s 76(2).

109 Serious Crime Act 2015, s 76(8). The burden rests with the defendant to produce sufficient evidence for the matter to be considered by the jury; it would then be for the prosecution to demonstrate to the criminal standard of proof, namely beyond reasonable doubt, that the defence has not been made out: see Serious Crime Act 2015 Explanatory Notes, [312].

110 Serious Crime Act 2015, s 76(10).

reasonable to cause someone serious alarm or distress that has substantial adverse effect on daily activities.[111]

8.106 The maximum penalty for the offence is five years' imprisonment on indictment and/or a fine.[112]

8.107 During the 2017-18 financial year, 960 offences of coercive control were charged and reached a first hearing.[113]

Public Order Act offences

8.108 Harassing conduct can also be pursued as either the offence of "intentional harassment, alarm or distress" or "harassment, alarm or distress" under sections 4A and 5 of the POA 1986. These offences do not require a "course of conduct" to be demonstrated, but cannot be committed where the conduct occurs exclusively within private dwellings.[114]

8.109 It seems relatively clear, following the case of *S v DPP*,[115] that the more serious of these offences – intentionally causing alarm or distress, can be pursued in an online context. However, it is not clear that the less serious section 5 offence, which requires the conduct to be "within the hearing or sight of a person likely to be caused harassment, alarm or distress thereby" can be committed online.[116]

8.110 While this superficially indicates a lack of parity between the online and offline environments, conduct of the kind referred to in section 5 of the POA 1986 offence could fall within one of the communications offences outlined in Chapter 4 and referred to again at paragraph 8.127 below.

Intentional harassment, alarm or distress – section 4A of the Public Order Act 1986

8.111 The offence of causing intentional harassment, alarm or distress was introduced into the POA 1986 by the Criminal Justice and Public Order Act 1994.

8.112 It is a more serious offence than the section 5 offence, and carries a maximum penalty of six months' imprisonment or a fine.[117]

8.113 The main difference between the two offences is that the section 4A offence is a "result crime", unlike the section 5 offence which is a "conduct crime". The section 4A offence requires some harm to have been caused, while the section 5 offences focuses on the

---

111 V Bettinson, "Criminalising Coercive Control in Domestic Violence Cases: Should Scotland Follow the Path of England and Wales" [2016] 3 *Criminal Law Review* 165, p 174.

112 Serious Crime Act 2015, s 76(11).

113 Crown Prosecution Service, *Violence Against Women and Girls Report 2017-18* (10th ed, September 2018) p A11, available at https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2018.pdf.

114 Public Order Act 1986, ss 4A(2), 5(2).

115 [2008] EWHC 438 (Admin); [2008] 1 WLR 2847.

116 *S v DPP* [2008] EWHC 438 (Admin); [2008] 1 WLR 2847 at [12] and [15].

117 Public Order Act 1986, s 4A(5).

behaviour of the perpetrator. The section 4A offence requires specific intention to cause a person harassment, alarm or distress and the actual causing of harassment, alarm or distress. It can also be committed by using "insulting" words or behaviour, or displaying any writing, sign or visual representation that is insulting.

8.114 There must be a causal connection between the conduct of the defendant and the effect on the victim.[118] However, in an online context, courts have found that a significant gap in time between when that offending conduct is posted online, and when it is viewed by the victim, does not necessarily break the chain of causation.[119]

Harassment, alarm or distress – section 5 of the Public Order Act 1986

8.115 The offence of harassment, alarm or distress is the lesser of the two harassment offences in the POA 1986. It carries a maximum penalty of a fine of £1000.[120]

8.116 It was the most controversial of the offences introduced by the POA 1986, and is used to prosecute a wide range of low-level anti-social behaviour,[121] such as verbal abuse between neighbours.

8.117 Its essential elements are that "within the hearing or sight of a person likely to be caused harassment, alarm or distress thereby" the defendant either:

(1) uses threatening or abusive words or behaviour, or disorderly behaviour; or

(2) displays any writing, sign or other visible representation which is threatening or abusive.[122]

8.118 Prior to 2013, the offence also extended to "insulting" words, however this language was removed following concern that this extended the reach of the offence too far.[123]

8.119 Whether a person is likely to be caused harassment, alarm or distress is a question of fact, dependent on the circumstances of the case. "Harassment" does not require apprehension about personal safety,[124] while distress requires some degree of emotional disturbance or upset.[125]

---

118 HHJ Thornton and others, *The Law of Public Order and Protest* (2010) p 46.

119 *S v DPP* [2008] EWHC 438 (Admin); [2008] 1 WLR 2847 at [13].

120 Public Order Act 1986, s 5(6).

121 HHJ Thornton and others, *The Law of Public Order and Protest* (2010) p 37.

122 Public Order Act 1986, s 1.

123 Crime and Courts Act 2013, s 57. See also also P Strickland and D Douse, *"Insulting words or behaviour": Section 5 of the Public Order Act 1986* (Standard Note SN/HA/560, 15 January 2013), available at http://researchbriefings.files.parliament.uk/documents/SN05760/SN05760.pdf.

124 *Chambers v DPP* [1995] *Criminal Law Review* 896.

125 *Southard v DPP* [2006] EWHC 3449 (Admin).

8.120 The fault element of the offence is that the person intends their words or behaviour, or the writing, sign or other visible representation, to be threatening or abusive, or is aware that it may be.[126]

Racial and religious aggravation of POA 1986 offences

8.121 If racially or religiously aggravated, either offence can be pursued as an aggravated offence under the Crime and Disorder Act 1998.[127] The maximum penalty for the section 4A offence increases to two years' imprisonment, and the section 5 offence increases to a £2500 maximum fine.[128]

Offence of harassment at home contrary to section 42A of the Criminal Justice and Police Act 2001

8.122 Another harassment offence that does not require a "course of conduct" is the offence of harassment at home contrary to section 42A of the Criminal Justice and Police Act 2001. This offence criminalises conduct where a person is present outside, or in the vicinity of, a person's residence, and seeks to persuade them to do or not do something, while having the intention to harass or to cause them alarm or distress, or where the person engaged in the conduct should know (by reference to the reasonable person) that it will harass or cause the other alarm or distress. The conduct must amount to harassment or cause alarm or distress of someone in or near the residence, or be likely to do so.

8.123 Unlike the PHA 1997 offence of harassment, which is a result crime, this offence is a conduct crime, as it can be committed in circumstances where the conduct "is likely to result in the harassment of, or to cause alarm or distress to, any such person",[129] even if it does not, in practice, result in harassment.

8.124 A key component of the offence is presence outside or in the vicinity of the dwelling. While the offence could have an online component – such as where the harasser is also sending abusive messages by email – the offence cannot be committed without this physical dimension.

8.125 The maximum penalty for this offence is six months' imprisonment.[130]

8.126 Crown Prosecution Service ("CPS") case management data indicates that in practice this charge is rarely pursued, and is not used for online offending.

---

126 Public Order Act 1986, s 6(4).

127 Crime and Disorder Act 1998, s 31(1)(b) and (c).

128 Crime and Disorder Act 1998, s 31(1)(b) and (4).

129 Criminal Justice and Police Act 2001, s 42A(1)(d).

130 Criminal Justice and Police Act 2001, s 42A(5) and (6).

Communications offences

8.127 Individual acts of harassment or stalking might also be pursued as communications offences under the MCA 1988[131] and the CA 2003.[132] These offences have already been outlined in detail in Chapter 4.

8.128 As Bakalis has noted, while the offence under section 1 of the MCA 1988 may be useful in certain cases of online harassment, the threshold of a "grossly offensive" communication is also limiting, as many acts that will constitute harassment will not meet this standard.[133]

8.129 Of particular note for present purposes is section 127(2)(c) of the CA 2003, which criminalises persistently making use of a public electronic communications network, for the purposes of causing annoyance, inconvenience or needless anxiety.

8.130 This is an exceptionally broad offence. Anyone who regularly uses the internet in order to, for example, annoy a work colleague, could theoretically commit the offence. It is a conduct crime; no harm needs to be caused, so the work colleague in this scenario need not even be caused any annoyance.

8.131 However, CPS guidelines are clear that the threshold for prosecution of these offences is high, and prosecution needs to be a proportionate response in the light of the protections on freedom of expression outlined in article 10 of the European Convention on Human Rights ("ECHR").[134]

8.132 An example of a section 127 offence being charged in a harassment context was the case of Caroline Criado Perez.[135] Ms Perez had led a successful campaign in 2013 to have a female figure depicted on a Bank of England note. She was then subjected to a series of abusive tweets by two perpetrators. The tweets sent anonymously by the first perpetrator were summarised by the sentencing judge as follows:

> Fuck off and die ... you should have jumped in front of horses, go die; I will find you and you don't want to know what I will do when I do… kill yourself before I do; rape is the last of your worries; I've just out of prison and would happily do more time to see you berried; seriously go kill yourself! I will get less time for that; rape? I'd do a lot worse things than rape you.

8.133 The offender pleaded guilty to a section 127(2) offence and was sentenced to 12 weeks' immediate custody.

---

131 Malicious Communications Act 1988, s 1.

132 Communications Act 2003, s 127.

133 C Bakalis, "Rethinking cyberhate laws" (2018) 27(1) *Information & Communications Technology Law* 86, p 98.

134 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (21 August 2018), available at https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (last visited 28 September 2018).

135 See *R v Nimmo and Sorley* (Sentencing Comments, 24 January 2014), available at https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/r-v-nimmo-and-sorley.pdf.

8.134 The second offender wrote a series of tweets which included the following:

> Ya not that gd looking to rape u be fine; I will find you; come to geordieland (Newcastle) bitch; just think it could somebody that knows you personally; the police will do nothing; rape her nice ass; could I help with that lol; that I cud do to u; dumb blond bitch.

8.135 The second offender also pleaded guilty to a section 127(2) offence and was sentenced to eight weeks' immediate custody.

Public nuisance

8.136 The common law offence of public nuisance has also been pursued in cases of harassing conduct, although we are not aware of any prosecutions for online behaviour.

8.137 The offence is defined in *Archbold* as follows:

> A person is guilty of a public nuisance (also known as common nuisance), who (a) does an act not warranted by law, or (b) omits to discharge a legal duty, if the effect of the act or omission is to endanger the life, health, property or comfort of the public, or to obstruct the public in the exercise or enjoyment of rights common to all Her Majesty's subjects.[136]

8.138 It is therefore very broad in scope, although there are now a wide range of statute-based offences that directly cover the various types of conduct criminalised by this offence (for example, the harassment and communications offences referred to in this Chapter, and various environmental laws that deal with other public nuisance conduct such as obstructing roads and dumping waste).

8.139 The offence was last considered in detail by the House of Lords in *R v Rimmington*,[137] which considered two conjoined appeals. Of most relevance was the first appeal, which related to a charge of:

> sending 538 separate postal packages … containing racially offensive material to members of the public selected by reason of their perceived ethnicity or for their support for such a group or randomly selected in an attempt to gain support for his views, the effect of which was to cause annoyance, harassment, alarm and/or distress.

8.140 In overturning the conviction for this offence, the House of Lords overturned previous authority, and found that the "the crime of public nuisance does not extend to separate and individual telephone calls, however persistent and vexatious, and the extension of the crime to cover postal communications would be a further illegitimate extension".[138]

---

136 M Lucraft (ed), *Archbold Criminal Pleading Evidence and Practice 2019* (2018) paras 31 to 40.

137 [2005] UKHL 64, [2006] 1 AC 459.

138 *R v Rimmington* [2005] UKHL 64; [2006] 1 AC 459 at [38].

8.141 More generally, the House of Lords found that much of the conduct that falls within the common law offence is now the subject of a statutory offence, and that:

> good practice and respect for the primacy of statute … require that conduct falling within the terms of a specific statutory provision should be prosecuted under that provision unless there is good reason for doing otherwise.[139]

8.142 The Law Commission considered this offence recently in our project on "Public Nuisance and Outraging Public Decency", where we recommended retaining the offence, but setting out its elements more clearly in statute.[140]

8.143 Given the wide array of statutory offences covering online harassment, it is difficult to see public nuisance being justifiably used in favour of these other offences in cases of online harassment and stalking.

PROSECUTIONS FOR HARASSMENT AND STALKING

8.144 The 2017 Crime Survey for England and Wales suggests that approximately one in five women and approximately one in 10 men have experienced stalking.[141] Police recorded incidents of stalking and harassment in England and Wales are roughly five reports per 1000 people.[142] Prosecutions were commenced for 11,922 stalking and harassment offences in 2017–18, 1616 of which were for stalking offences.[143] There were also a further 17,012 prosecutions for breach of restraining orders made under the PHA 1997.[144] The majority (73.3%) of prosecutions under all these offence types were flagged by the CPS as domestic abuse related.[145]

---

139 *R v Rimmington* [2005] UKHL 64; [2006] 1 AC 459 at [30].

140 Simplification of Criminal Law: Public Nuisance and Outraging Public Decency (2015) Law Com No 358, pp 78 to 79.

141 Office for National Statistics, *Domestic abuse in England and Wales: year ending March 2016* (December 2016), available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/domesticabuseinenglandandwales/yearendingmarch2016.

142 Office for National Statistics, *Crime in England and Wales: year ending December 2017* (April 2018), available athttps://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2017.

143 Crown Prosecution Service, *Violence Against Women and Girls Report 2017-18* (10th ed, September 2018) p A20, available at https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2018.pdf.

144 Crown Prosecution Service, *Violence Against Women and Girls Report 2017-18* (10th ed, September 2018) p A20, available at https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2018.pdf.

145 Crown Prosecution Service, *Violence Against Women and Girls Report 2017-18* (10th ed, September 2018) p A20, available at https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2018.pdf.

8.145 It is not possible to distinguish further the proportion of these charges that are committed online, and as we have noted, a "course of conduct" may involve a mixture of online and offline behaviours.

8.146 One of the issues with PHA 1997 offences is that the totality of a series of seemingly low-level incidents may be misinterpreted by police and prosecutors, and the appropriate harassment or stalking charges will not be pursued.[146] Similar challenges are also present in demonstrating that the offender has "repeatedly or continuously" engaged in controlling or coercive behaviour for the purposes of the offence under section 76 of the Serious Crime Act 2015.[147]

8.147 A 2017 joint report by the police and CPS inspectorate bodies was critical of the police and CPS response to harassment and stalking. The report found there was a lack of understanding of the offences, and that victims' concerns were not being adequately addressed.[148] In response, the police and CPS have committed to implementing a series of reforms, including the release of an updated joint working protocol.[149]

Alternatives to criminal prosecution

8.148 Not all allegations of stalking and harassing conduct will result in prosecution. Other avenues that may be pursued to prevent further conduct are outlined below.

Police information notice – early intervention

8.149 As an early response to stop further harassment, police sometimes issue "police information notices" ("PINs") to alleged perpetrators. These notices are not formal cautions, but serve to warn suspects that their alleged actions may constitute an offence. They may be appropriate to prevent further stalking or harassment where a course of conduct has not yet been established, or there are other difficulties in pursuing a prosecution. The issue of such a notice may also form part of evidence used in a future case against the recipient.

8.150 The issue of such a notice was challenged in *Hewson v Commissioner of Police of the Metropolis*, where it was argued that a notice warning a barrister about making disparaging tweets about another barrister infringed her rights to private life (Article 8) and freedom of expression (Article 10) of the ECHR.[150] However, while the High Court found that the notices did indeed interfere with her Article 8 and 10 rights, the interference was held to be proportionate in the circumstances.

---

146 E Finch, *The Criminalisation of Stalking: Constructing the Problem and Evaluating the Solution* (2001).

147 Indeed, there can be significant overlap between the offences in domestic abuse contexts. The coercive and controlling behaviour offence is considered more appropriate in cases where it occurs in the context of an ongoing relationship between the victim and the perpetrator.

148 HMIC and HMCPSI, *Living in fear - the police and CPS response to harassment and stalking* (2017) https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/living-in-fear-the-police-and-cps-response-to-harassment-and-stalking.pdf.

149 Crown Prosecution Service, *Action on Stalking and Harassment* (23 May 2018), available at https://www.cps.gov.uk/cps/news/action-stalking-and-harassment.

150 *Hewson v Commissioner of Police of the Metropolis* [2018] EWHC 471 (Admin); [2018] 4 WLR 69.

8.151 The 2017 joint inspectorate report referred to at 8.147 recommended that Chief Constables should stop the use of PINs and their equivalents immediately, finding that they act as a potential barrier to effective investigation of stalking.[151] The College of Policing is currently updating its guidance for police officers on stalking and harassment, which includes consideration of the ongoing use of PINs.

Non-molestation orders under the Family Law Act 1996

8.152 Where the alleged perpetrator is associated with the victim (generally meaning either they were in a relationship or are related),[152] that person may apply for a non-molestation order under section 42 of the Family Law Act 1996. The Family Court can issue an order prohibiting certain conduct by the subject of the order.

8.153 In deciding whether to make a non-molestation order, and the form it should take, the court must have regard to all the circumstances including the need to secure the health, safety and well-being of the applicant and any relevant child.[153]

8.154 Non-molestation orders are civil orders, but breach of a non-molestation order is an offence with a maximum penalty of five years' imprisonment.[154]

Injunctions under the PHA 1997

8.155 A person who is or may be a victim of harassment or stalking can apply for an injunction to prevent another person from engaging in certain conduct.[155] These are different to the restraining orders referred to above, as they do not require a criminal prosecution, and apply in circumstances of "actual or apprehended" harassment.

8.156 A breach of a civil injunction made under the PHA 1997 carries a maximum penalty of five years' imprisonment.[156]

Stalking Protection Bill

8.157 A Bill currently before Parliament – the Stalking Protection Bill – would allow the police to apply for a "stalking protection order" in circumstances where it appears that a person has carried out acts associated with stalking, that they pose a risk associated with stalking to another person, and that an order is necessary to prevent against that risk.[157]

8.158 Under the proposals, a breach of such an order would be punishable by up to five years' imprisonment.[158]

---

151 HMIC and HMCPSI, *Living in fear - the police and CPS response to harassment and stalking* (2017) pp 48 to 49, available at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/living-in-fear-the-police-and-cps-response-to-harassment-and-stalking.pdf.

152 For a full definition see Family Law Act 1996, s 62(3).

153 Family Law Act 1996, s 42(5).

154 Family Law Act 1996, s 42A(5)(a).

155 Protection from Harassment Act 1997, ss 3, 3A.

156 Protection from Harassment Act 1997, s 3(9).

157 Stalking Protection Bill, cl 1.

158 Stalking Protection Bill, cl 8(2)(b).

8.159 At the time of writing, this Bill was at the committee stage in the House of Commons, and had not yet been before the House of Lords.

ONLINE HARASSMENT AND CYBERSTALKING

Particular challenges of pursuing harassment and stalking offences committed online

8.160 As well as facilitating new and damaging forms of harassment and stalking, the online environment poses particular challenges for the law when seeking to hold individuals to account for their conduct under stalking and harassment offences.

8.161 Below we consider examples to illustrate some of these issues, which we have grouped under the following categories:

(1) The broad definition of harassment: is harassment online treated in the same way as harassment in person? Should the harasser escape liability if the target does not become aware of the harassment?

(2) The distinction between harassment and stalking: should the misuse of personal information that the victim has themselves posted online elevate a harassment to stalking?

(3) Defining a course of conduct for the purposes of the offence: can a single act that sets in train ongoing harassment amount to a course of conduct?

(4) Defences to harassment: do the defences and limitations in the offence provisions extend to online harassers and stalkers, and apply as they do offline?

(5) Anonymous harassment: how can the law deal effectively with harassers who cannot be identified?

8.162 A particular issue that we consider in more detail at paragraph from 8.195 below is the phenomenon of group, or "pile on", abuse of an another online. Participants at our stakeholders' experiences event and technology companies have told us this is an issue of real concern, due to its prevalence and the degree of harm that it causes. It is not clear that the current criminal law adequately addresses the particular harms and wrongs involved in this offending.

Defining harassment: is harassment online treated in the same way as harassment in person?

8.163 While there is no legal distinction between online and offline harassment, there can be differential treatment in practice, which reflects the often different standards of behaviour applied online and in person.

8.164 Participants in our stakeholders' experiences event expressed concern that there was a significant degree of inconsistency in how seriously police treated online abuse and harassment across the country, stating that sometimes there was something of a "postcodelottery".

Example 1: Twitter trolling

Gemma is a well-known campaigner for women's rights in the United Kingdom. She has a huge following on Twitter (@gemsrights) where she has over 10,000 followers and posts regularly about political, legal and social developments pertaining to women in the United Kingdom. Jordan is a follower and grows intensely to dislike her because of her political persuasions and perspectives. For a number of weeks, he responds to every tweet that Gemma posts, and generally insults her intellectual capabilities after every one of her tweets. The following are an example of some of his tweets:

> @gemsrights hasn't got a clue.
>
> @gemsrights must be the dumbest person I know.
>
> @gemsrights did you even go to university?
>
> @gemsrights fuck off and die already. I'm so sick of you and your inane rants."

Gemma becomes increasingly upset by his comments, but hopes that if she ignores him he will stop.

Analysis

8.165 If someone consistently made such comments to another in person (for example, in a work environment), it would be likely to be treated fairly seriously and considered to be harassing behaviour – probably not as a criminal matter, but as a serious employment disciplinary matter. However, in the online context, celebrities and public figures will be very accustomed to (though no doubt still affected by) messages of this sort from random strangers. Sadly, anyone posting publicly in a medium and context where members of the public can respond may now even come to expect rude and unwelcome criticism and comments. Nevertheless, the types of messages in the above example may constitute the offence of harassment when taken together.

8.166 Jordan has pursued a course of conduct, which amounted to the harassment of Gemma, as it caused her distress. There is a strong argument that he knew or ought to have known that the course of conduct amounted to harassment, though he may try to argue that he did not expect her to read the tweets, given how many followers she has. It appears then, that this could be an offence whether it was said to Gemma in person every day, or committed over the internet in this way. However, a significant concern remains that law enforcement agencies do not consistently treat harassing conduct equally seriously if it is committed solely in the online environment.

Should the harasser avoid liability if the target does not become aware of the harassment?

8.167 Another issue that can arise in online contexts, where individuals can have thousands of "followers" on social media, is that the "victim" of the harassment may not even realise it is happening.

Example 2: "victim" does not realise they are being harassed

In this example, the facts are the same as in Example 1. However, here, Gemma never actually reads any of the messages from Jordan. She decides that with so many followers, and with so many posting vile and insulting comments about her, she will not read or follow what others say about her. Jordan also attacks a number of Gemma's followers who state on their Twitter profile that they support women's rights. He sees another Twitter user (@tuurminate) has been posting the message: "you're a despicable piece of shit. Just shut up" to a number of Gemma's followers. Jordan retweets each message, "tagging" each of the followers and adding "Agreed. Fuck off already."

Another Twitter follower notices the fact that Jordan has targeted Gemma, and a quick browse of Jordan's Twitter page confirms that he almost exclusively comments negatively about her and her followers. He reports the messages to the police.

Analysis

8.168 For the offence of harassment to have been committed, the course of conduct must "amount" to the harassment of a person. Here, Gemma does not actually experience harassment as she never read any of the tweets, so a fundamental element of the offence of harassment of another has not been satisfied.[159]

8.169 An alternative in this circumstance would be a charge under section 127(1) of the CA 2003 on the basis that the posts are of a menacing character or grossly offensive. Unlike the PHA 1997 offences, these are conduct crimes, and do not require harm to be caused to the victim for the offence to be satisfied.

8.170 Furthermore, other followers of @gemsrights who do see the tweets and who were targeted by Jordan might feel harassed by the tweets. For Jordan to commit an offence under section 2 of the PHA 1997 on this basis, it would be necessary to show that he "knows or ought to know" that his conduct involves harassment of those persons.

The distinction between harassment and stalking

8.171 The introduction of the offence of stalking signalled the seriousness with which this form of harassment was to be treated by the law.[160] However, as "stalking" lacks an overarching definition, it is not always clear when harassing conduct has crossed the threshold into stalking. The following example illustrates the particular challenges that social media pose in this regard.

---

159 Protection from Harassment Act 1997, s 1(1)(a) and s 7(2). See also *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233; [2002] Entertainment and Media Law Reports 4 at [30].

160 However, in practice, the maximum penalty is currently the same as the offence of harassment as they are both summary offences.

Example 3: can accessing information a person has published on social media amount to stalking?

Tom and Jack meet in a bar through a mutual acquaintance. Jack immediately takes an interest in Tom, and learns where he works in a conversation they have that night. The next day, Jack finds Tom's email address from his work website, and asks him out for a drink. Tom refuses because he is in a serious relationship, but Jack won't take no for an answer and sends 20 emails over the course of a week. These range from the short and banal ("can't stop thinking about you") to more alarming messages, telling Tom that his current partner is not worthy of him.

Tom is also a prolific Facebook user, and his privacy settings are such that many of his posts are publicly available. Throughout the period that Jack was emailing Tom, he also repeatedly checks Tom's Facebook timeline, and references Tom's Facebook posts in his emails.

Analysis

8.172 The above scenario amounts to the offence of harassment under section 2 of the PHA 1997, as Jack's repeated messaging is a course of conduct which is "oppressive and unreasonable"[161] and which Jack at least ought to know could amount to harassment of Tom.

8.173 What is less clear is whether the conduct, and in particular Jack's monitoring and reciting of Tom's Facebook updates, amounts to stalking, contrary to section 2A of the PHA 1997.

8.174 Arguably, stalking is also committed here, even though monitoring of social media is typically expected and consented to within social media environments. But Jack has been "monitoring" a form of electronic communication (section 2A(3)(d)) which is an example of stalking behaviour in the PHA 1997.

8.175 The modern online context thus raises potential problems for determining the line between harassment and stalking. Online platforms have encouraged a sharing economy that has resulted in the "privacy paradox", where users care about their privacy online, but do not apply these concerns to their corresponding usage behaviour. Individuals may "befriend" strangers on social media only to gain a higher "friend" count, and may share intimate aspects of their lives with thousands of followers on social media. It is expected that "friends" and "followers" will have access to this information, and even to "monitor" the posts in these networks of "friends" or "followers". But where this rather unobtrusive conduct is now coupled with a course of conduct that constitutes harassment, a serious offence will be committed.

[161] *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233; [2002] Entertainment and Media Law Reports 4 at [30].

What is a "course of conduct" in an automated environment

8.176 The case law interpreting the meaning of a "course of conduct" assumes more than one act is committed by the defendant. However, what is less clear is whether a single act that sets in train a "course" of harassment over time falls within the current offence. Such "automated" harassment can be facilitated through technology online.

> **Example 4: what does a "course of conduct" mean in an automated environment?**
>
> John and Mary have had a falling out at work, and John is now intensely annoyed by Mary and everything she does in the office. He decides it would only be fair for her to be as annoyed as he is during her working day, so he accesses the "Darkweb" and from there purchases an "email bombing" service. This product guarantees that the victim will receive 10,000 emails in the first day, and that this will continue until the victim individually unsubscribes to each contact address. He pays $20 and subscribes Mary's work email address accordingly.

Analysis

8.177 This is potentially quite a serious offence, under section 3 of the Computer Misuse Act 1990, of intentionally or recklessly impairing the operation of a computer.[162]

8.178 However, if harassment were to be charged, the question raised by the example is whether one physical instance of "conduct" (sending an email address to a nefarious actor, and paying for the "service") could become a course of conduct due to the automated response which continuously bombards the victim with emails, no doubt causing great distress.

8.179 In *Kelly v DPP*,[163] the making of three telephone calls within five minutes of each other was held to be capable of constituting a "course of conduct" for the purposes of the PHA 1997, since it involved conduct on "at least two occasions". The fact that the recipient heard them all on the same occasion (when she accessed her voicemail) was considered irrelevant to this issue.

8.180 But it is not clear whether the reverse is true – does that offence apply to one instance of conduct resulting in multiple experiences of harassment by a victim? As a noun, the word "conduct" would certainly refer to the manner in which John behaves, but would it also cover the manner in which the activity (email bombing) takes place? It is not clear that this would be an offence under the PHA 1997. However, some support for this suggestion may be derived from the case of *Ferguson v British Gas Trading Ltd*, where computer generated demands for payment of utility bills were accepted as capable of amounting to a "course of conduct" for the purposes of a civil harassment claim.[164]

---

162 See *DPP v Lennon* [2006] EWHC 1201 (Admin); (2006) 170 JP 532 for a similar case in which section 3 was successfully charged.

163 [2002] EWHC 1428 (Admin); [2003] *Criminal Law Review* 45.

164 *Ferguson v British Gas Trading Ltd* [2009] EWCA Civ 46; [2010] 1 WLR 785 at [11].

8.181 A further alternative offence that might be pursued in this circumstance is the offence of persistently making use of a public electronic communications network, for the purposes of causing annoyance, inconvenience or needless anxiety, contrary to section 127(2)(c) of the CA 2003.

Harassment defences

8.182 There are a number of defences available for harassment offences, including that the conduct was reasonable in all the circumstances, and that it was pursued for the purpose of preventing or detecting crime.[165] This raises particular issues given the growth in online vigilante groups who seek to police the conduct of others online.[166]

Example 5: Paedophile vigilante group

Juan is a member of an online paedophile hunter group.

One of the activities the group engages in is collecting publicly available images of convicted paedophiles (from newspaper reports etc) and disseminating these pictures widely online once the perpetrator is released from prison, together with other information that is known about them. The group's intention in doing this is to protect members of the public from potential future abuse.

After a complaint to police by one of these released prisoners, Juan is investigated for harassment contrary to section 2 of the PHA 1997.

In his defence he claims he published the details for the purpose of preventing crime, and therefore the defence under section 1(3)(a) of the PHA 1997 is available.

Analysis

8.183 Online vigilante groups are common, and there have been high profile cases that have considered the legality of their conduct.[167]

8.184 Assuming that Juan's conduct in disseminating the pictures and information was found to be a course of conduct that amounted to the harassment of the prisoner, it is unlikely that a court would find that Juan's conduct was sufficiently connected to preventing a

165 Protection from Harassment Act 1997, s 1(3).

166 *Hayes v Willoughby* [2013] UKSC 17; [2013] 1 WLR 935 at [13].

167 See, eg, the Northern Ireland case of *CG v Facebook, Joseph McCloskey* [2015] NIQB 11. See also the recent case of *R v TL* [2018] EWCA Crim 1821, which considered whether a prosecution based on evidence collected by a vigilante group was an abuse of process. The Court of Appeal overturned a finding that it was, but added: "in reaching this conclusion we do not seek to undermine or contradict the stated position of the police, by which they discourage private individuals from setting out to identify those who groom children and arrange to meet them for sexual purposes. They have concerns that their own investigations might be compromised, that private investigations may not produce admissible evidence, that there may be risks to the safety of the investigators and the subjects of their investigations and that the zeal of some "vigilantes" may lead them to seriously improper conduct" at [39].

crime, even if he genuinely believed that he was doing so.[168] By potentially damaging the rehabilitation of an offender, his conduct might even have the opposite effect.

Anonymous harassment

8.185 A particular feature of online harassment is that the identity of the perpetrator may not be known to the victim, and can prove difficult for law enforcement to track down. This creates practical challenges in seeking to address the conduct effectively through the criminal law.

Example 6:

May is a student, who also does modelling work part time to support her studies. She has an online presence and her contact details are easily ascertainable.

She begins to receive a series of anonymous abusive text messages and phone calls.

Soon after the calls begin she discovers that a website has been set up which contains explicit and untrue statements about her sex life. She recognises the tone and content of the website as being consistent with that of the abusive calls and messages she has been receiving.

May contacts the police to try and put a stop to the conduct, but their investigation is unable to determine the identity of the perpetrator.

Analysis

8.186 The legal response to such anonymous harassing conduct has been considered in the recent case of *GYH v Persons Unknown*,[169] where the claimant applied without notice to the defendant for an interim non-disclosure order to restrain a campaign of harassment by the (unknown) defendant. The Court noted the availability of civil remedies where a claimant cannot identify those responsible for the conduct complained of,[170] but also the need to "guard against any abuse of the facility".[171]

8.187 The High Court noted in particular, that section 12(2) of the Human Rights Act 1998 prohibits the court from granting relief which might affect the exercise of the ECHR right to freedom of expression unless it is satisfied "that there are compelling reasons why

168 See *Hayes v Willoughby* [2013] UKSC 17; [2013] 1 WLR 935 at [13].

169 [2017] EWHC 3360 (QB).

170 See further *Bloomsbury Publishing Group plc v News Group Newspapers Ltd* [2003] EWHC 1205 (Ch); [2003] 1 WLR 1633.

171 *GYH v Persons Unknown* [2017] EWHC 3360 (QB) at [10].

the respondent should not be notified or that the applicant has taken all practicable steps to notify the respondent".[172]

8.188 The Court also noted that in the absence of any respondent to the application it must be vigilant in identifying and giving appropriate weight to any point of fact or law that might be said to count against the grant of the relief sought.[173]

8.189 For May to seek civil relief in this case, she would therefore need to demonstrate that she had taken reasonable steps to identify and notify the defendant. In presenting the case, she would need to comply with a duty of full and frank disclosure of all pertinent details to the court, including those which might count against her.

8.190 Other options open to May to enforce the withdrawal of the offending material include the right to rectification and right to erasure under sections 46 and 47 of the Data Protection Act 2018. She might also request that Google remove the offending websites from the search by making use of its Personal Information Removal Request Form.[174]

8.191 While there are avenues for May to enforce the takedown of the offending material, in terms of holding the perpetrator criminally responsible, the practical challenges of identifying and thereby enforcing sanction against them remain.

Example 7:

Anna is a single woman and makes regular use of online dating apps.

She starts to receive very unpleasant, sexually explicit messages from a user across these various platforms.

Anna tries to block the user, but they keep reappearing via new accounts.

This causes Anna to withdraw from online dating, which used to be an important part of her social and relationship life.

8.192 Offensive and abusive messaging on online dating applications has emerged as an increasing problem in recent years.

8.193 The conduct of the anonymous user in this example is quite likely to amount to the harassment of Anna, as well as an offence under section 1 of the MCA 1988 or section 127 of the CA 2003.

---

172 *GYH v Persons Unknown* [2017] EWHC 3360 (QB)

173 *GYH v Persons Unknown* [2017] EWHC 3360 (QB) at [28].

174 See Google, *Personal Information Removal Request Form* (2018), available at https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf.

8.194 There is no obvious legal impediment to this conduct being pursued. However, it is likely that the prosecution would face a number of practical challenges in seeking to hold the perpetrator to account. These might include:

(1) the difficulty in gathering the evidence, particularly where it is strewn across a number of different accounts and platforms; and

(2) the difficulty in identifying the perpetrator, particularly where very few personal details are required to establish an account.

Group harassment

8.195 Earlier in this Chapter, we considered section 7(3A) of the PHA 1997 which was introduced to address campaigns of harassment by a group.

8.196 Below, we consider the ways in which the online environment can facilitate group harassment, the harm that it can cause, and the extent to which it is adequately dealt with by the current law.

Drivers of group offending online

8.197 While "ganging up" against another is not a uniquely online phenomenon, the internet facilitates this kind of behaviour in a number of ways, which we explore in further detail in Chapter 2.

8.198 In practical terms, the internet provides an easier forum for group offending than the offline context:

(1) the defendant is more likely to find like-minded people who share a desire to communicate in an offensive or abusive way;[175]

(2) it is easier to identify, locate and target the victim, or someone with the characteristics of the victim; and

(3) if an organised group is established, technology enables easy co-ordination of that group.[176]

8.199 From a psychological standpoint, there are also a number of aspects of the online environment that motivate or enable participation in group abuse:

(1) The defendant/s benefit from the disinhibiting effect of being part of a group where the victim is often unseen and geographically remote. This can lead offenders to feel emboldened to act and disengaged from the consequences of their behaviour.

---

175 E Rutger Leukfeldt, ER Kleemans, WP Stol; "Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing and Malware Networks" (1 May 2017) 57(3) *The British Journal of Criminology* 704, p 704.

176 J Banks, "Regulating Hate Speech Online" (November 2010) 24(3) *International Review of Law, Computers & Technology* 233.

(2) The defendant may also feel emboldened to act as part of the group by the perception that he or she is anonymous online, both to the victim and to other offenders.[177]

What kinds of harm are caused by group harassment

8.200 As we note in Chapter 3, the harm caused to victims of online abuse, including group attacks, can take many forms, including psychological and economic detriment. Charities who work in this field have provided examples of people who have committed suicide after being targeted by group attacks online. We have also heard that the effects of group offending have a "ripple effect"; impacting upon not only the victim themselves, but on other people online, who see the offending behaviour and are fearful that it could happen to them.

8.201 Users have described how abuse coming from a group of people has an exacerbated impact, due to its unremitting nature. In one well-documented instance, Jess Phillips MP reported receiving 600 "negative rape threats" of "I would not rape you" in one evening.

8.202 Other users have spoken to us about the impact of receiving repetitive, abusive messages which singly would not have caused them harm.

8.203 This leads us to conclude that there is a distinctive harm involved in being a victim of a group abuse online.

Current law concerning group harassment

8.204 As we have seen, the law caters for online abuse or harassment by one person of another in a number of ways:

(1) in the case of a single instance of abuse by one defendant against a single victim, a communications offence or public order offence may apply; and

(2) where the defendant has committed multiple instances of abuse, an offence under the PHA 1997 might also be available.

8.205 Amendments to the PHA 1997 have also been introduced to cater for certain other scenarios involving multiple victims or multiple defendants:

(1) the harassment of a group by a single defendant, through at least one incidence of conduct by the defendant against each of two or more group members;[178]

(2) collective offending, where a defendant has aided, abetted, counselled or procured one or more other persons to harass a victim;[179] and

---

177 DK Citron, "Cyber Civil Rights" (2009) 89 *Boston University Law Review* 61.

178 Protection from Harassment Act 1997, s 1(1A).

179 Protection from Harassment Act 1997, s 7(3A).

(3) collective group offending, where a defendant has aided, abetted, counselled or procured one or more other persons to harass a group.[180]

8.206 Further, as we note in Chapter 12, which considers inchoate liability, a defendant who encourages or assists another to commit a communications or harassment offence, could also potentially be held criminally liable under the broad terms of sections 44 to 46 of the Serious Crime Act 2007. This liability would be irrespective of whether the communications or harassment offence is committed.

8.207 Despite the availability of these various forms of principal, secondary and inchoate liability, in practice, it appears that the criminal law is having little effect in punishing and deterring certain forms of "group" abuse, notably:

(1) the coordination of a campaign of abuse (for example, through posting on a web forum or social media group with the intention of inciting others to send abusive messages to a victim);

(2) an agreement to undertake a campaign of abuse (for example, a decision by members of a particular political group to target an opponent with a torrent of abusive messages); and

(3) the conduct of a person in sending a single abusive message, but doing so in the knowledge that:

(a) similar abuse is being targeted at the victim (whether arising from a deliberate campaign or spontaneously); and

(b) an awareness of the risk of greater harm to the victim occasioned by their conduct in these circumstances (for example, the example referred to above where hundreds of individuals sent Jess Phillips MP "I would not rape you" messages).

8.208 There is therefore arguably a mismatch here between the forms of harm that are occurring online, and the response of the criminal justice system to them.

[180] Protection from Harassment Act 1997, ss 1(1A), 7(3A).

Example 8: coordinated abuse

Marina (@Marina98) is a student, and also an active participant in Conservative politics. She is strongly opposed to social welfare, and writes regularly in favour of "personal responsibility" rather than "government handouts".

Marina's views infuriate Joseph, who is also active on a left-wing web forum. He decides he wants to silence Marina as he considers her views damaging to society. After setting out the reasons for his opposition to Marina, he posts the following on the forum:

> Her views are intolerable and we need to shut her down. Let's send @Marina98 one of the following:
>
> "No one wants to hear your entitled bullshit you heartless bitch"
>
> "I hope you end up in the gutter one day so we can stomp you down"
>
> "You know exactly where you can shove your fucking privilege"

This leads to hundreds of abusive messages flooding Marina's Twitter account, and her other social media platforms.

Marina is so startled and scared by this wave of abuse that she shuts down all her social media accounts, and withdraws from all involvement in politics.

Analysis

8.209 In this scenario, it is possible that the various individuals who have sent Marina a message could have committed an offence under section 1 of the MCA 1998 or section 127 of the CA 2003. Joseph could also be liable as an accessory under section 44 of the Magistrates' Court Act 1980, or because he "caused" the message to be sent.[181]

8.210 However, while cumulatively the messages have had a devastating impact on Marina, it is not clear that the content of any one of these messages is of sufficient gravity that such a charge would be pursued against the sender.

8.211 For this reason, it may also be difficult for Joseph to be held liable for encouraging the commission of an offence under the Serious Crime Act 2007, as the conduct he has encouraged would not amount to an offence by any of the individual perpetrators.

8.212 Another option available would be a charge against Joseph for harassment contrary to section 2 of the PHA 1997, relying on section 7(3A) to establish that he has committed a "course of conduct" through aiding, abetting, counselling or procuring others to send the abusive messages (the "conduct") that amounts to harassment of Marina.

[181] Malicious Communications Act 1988, s 1(3); Communications Act 2003, s 127(1)(b).

8.213 While technically available to a prosecutor, the complex legal and evidential issues involved in pursuing such a harassment claim (which we outline in more detail at paragraphs 8.39 to 8.48 of this Chapter) are likely to act as deterrent to pursuing such a prosecution in practice. This is particularly so given that the offence is a summary only offence.

CONCLUSION

8.214 Our review of the applicable law in this Chapter has shown that there are a wide variety of offences that may pursued in cases of online stalking or harassment.

8.215 In fact, as we have noted elsewhere in this Report, one of the challenges for police and prosecutors is navigating the array of potential harassment and stalking, public order and communications offences that might be applicable. However, this can be addressed to some extent through clear prosecutorial guidance.

8.216 Superficially at least, there is also no reason why the main harassment offences could not apply equally to online or offline conduct, and they are indeed pursued in these contexts. However, as we have seen in other contexts, there can be technical and resourcing challenges in gathering evidence in circumstances where harassers and stalkers have taken steps to cover their tracks online.

8.217 There is sometimes also a perception that online harassment and stalking is not as serious as its offline equivalents, and that victims have options such as "blocking" perpetrators or disengaging with certain platforms. A participant in our stakeholders' experiences event responded to this as follows:

> when someone is fixated on you they will find a way to you; if you shut down your Facebook they will go to Twitter, if you remove your online presence they will find you offline.

8.218 Another participant added:

> removing yourself from the online world is extremely isolating. Online is a public space and can often be an extension of who we are.

8.219 We do not consider that the onus should ever be placed on the victim to modify their behaviour in relation to online abuse; though undoubtedly victims often do so.

8.220 One area which the substantive criminal law arguably does not adequately address at present is the phenomenon of group or "pile on" harassment of an individual. Harassment offences and prosecutions at present are primarily targeted at repetitive, oppressive conduct by an individual against another individual or group. However, where multiple people commit single acts of abuse against another – either spontaneously, following collective agreement, or incitement/coordination by a particular individual – that conduct can easily "amount to" harassment or stalking of the victim.

8.221 While the PHA 1997 does have a mechanism available to deal with collective harassment, it appears to be poorly understood and overly complex.

8.222 An issue which we consider worthy of further, detailed enquiry is whether specific offences of inciting, coordinating or participating in group harassment might be considered, so that they can be used to describe more effectively and punish this damaging form of abuse.

Chapter 9: Hate crime online

INTRODUCTION

9.1 It is an unfortunate fact that hostility towards certain groups in society remains prevalent in the online environment, as indeed it does offline.[1] In this Chapter we consider the hate crime laws that apply to online abusive and offensive communications. In September 2018, the Government announced that it will be asking us to conduct a separate, wider review of hate crime laws in England and Wales,[2] and many of the issues that we identify in this Chapter are likely to be relevant to this broader review.

The scale and challenge of online hatred

9.2 The online environment provides an additional, and powerful forum for hate crime offending. The volume of hateful language used online is enormous. For example, the website "NoHomophobes.com" records that the word "faggot", a derogatory term often targeted at gay men, has been used over 39 million times on Twitter globally since 2012.[3] Moreover, the 2016 Galop LGBT+ survey found that 84% of respondents had experienced at least one incidence of online abuse.[4]

9.3 Similarly, 2016 research commissioned by The Guardian into the 70 million comments left on its site since 2006, discovered that of the 10 writers abused most in comments, eight were women, and the remaining two were black men.[5]

9.4 At our stakeholders' experiences event, participants described to us the wide array of abuse that occurs online in respect of race, religion, sexual orientation, disability, gender, transgender status and political views. This is consistent with the findings of the Home Affairs Committee's "Hate crime and its violent consequences inquiry", which released a damning report on "abuse, hate and extremism online" in 2017.[6]

9.5 Indeed, it is not difficult to find clear expressions of such hatred online. Some of it may be targeted at certain individuals based on who they are, while other examples will incite or reinforce hatred against entire communities.

9.6 Most directly, the online environment facilitates hate crime by providing a means by which huge audiences can easily be reached, amplifying its effect.

---

1 We explore the harm that this causes in greater detail in Chapter 3.

2 *Hansard* (HC), 5 September 2018, vol 646 col 280.

3 See http://www.nohomophobes.com/!/all-time/.

4 M Stray, *Online Hate Crime Report 2017: Challenging online homophobia, biphobia and transphobia*, p 2, available at http://www.galop.org.uk/wp-content/uploads/2017/08/Online-hate-report.pdf.

5 B Gardiner and others, *The dark side of Guardian comments* (12 April 2016), available at https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments.

6 Hate crime: abuse, hate and extremism online: Government Response to the Committee's Fourteenth Report of Session 2016 – 2017 (2017) Cm 9566.

9.7 This means that in addition to any "intended" recipients, hate speech may also impact negatively on other witnesses to the speech, including members of the affected group, and even those beyond it.[7]

9.8 There is also evidence to suggest that perpetrators of online hate speech can incite each other, and push people to act on their hatreds including by using violence.[8]

9.9 The anonymity (real or perceived) and the disinhibiting effect of the internet, that we have discussed in greater detail in Chapter 2, can also contribute to people saying and doing things online that they might not do in person in a communication offline. This might include explicit hate speech.

Hate crime in the criminal law of England and Wales

9.10 The term "hate crime" in the law of England and Wales broadly refers to a range of criminal behaviour where the defendant is motivated by hostility or demonstrates hostility towards a victim based on certain characteristics.[9] The definition adopted by the Crown Prosecution Service ("CPS") and the National Police Chiefs' Council for hate crime is:

> any criminal offence which is perceived by the victim or any other person, to be motivated by a hostility or prejudice based on a person's race or perceived race; religion or perceived religion; sexual orientation or perceived sexual orientation; disability or perceived disability and any crime motivated by a hostility or prejudice against a person who is transgender or perceived to be transgender.[10]

9.11 As can be seen from this definition, in England and Wales, the characteristics to which hate crime offending apply are race, religion, disability, sexual orientation and transgender identity. However, there is inconsistency as to how these groups are treated across the criminal law, with certain hate crimes existing in respect of some of these characteristics, but not others.[11] There are also other characteristics such as age and gender that are protected in other contexts,[12] but not in the context of hate crime laws.

---

7 C Bakalis, "Rethinking cyberhate laws" (2018) 27(1) *Information & Communications Technology Law* 86, p 104.

8 See, eg R Cohen-Almagor, "Taking North American White Supremacist Groups Seriously: The Scope and Challenge of Hate Speech on the Internet" (2018) 7(2) *International Journal for Crime, Justice and Social Democracy* 38, p 47.

9 However, the offences of "stirring up" hatred have a related but different emphasis, and focus on the encouragement of hatred towards a particular a racial or religious group or sexual orientation.

10 See Crown Prosecution Service, *Hate Crime Strategy: 2017-2020*, available at https://www.cps.gov.uk/sites/default/files/documents/publications/CPS-Hate-Crime-Strategy-2020-Feb-2018.pdf.

11 For further discussion of this see, Hate Crime: Should the Current Offences be Extended? (2014) Law Com No 348.

12 See, eg Equality Act 2010, s 4.

9.12 This partly reflects the historical development of hate crime laws, which have emerged in a somewhat piecemeal fashion over decades, rather than as a single coherent body of law.

9.13 While there are many common features of hate crime, this offending does not affect all groups in the same way. For example, there is evidence to suggest that hate crimes based on sexual orientation are more likely to be characterised by violence. Moreover, disabled hate crime victims are more likely to be the targets of property and sexual offences.[13]

9.14 There are also different degrees of hostility that might underlie offending, varying from mild dislike or suspicion to deep seated hatred.[14]

The significance of hate crime laws in an online context

9.15 In this Chapter we consider the three main ways in which hate crime is targeted in the criminal law of England and Wales:

(1) offences of incitement/stirring up of hatred offences, which apply to race, religion and sexual orientation (Public Order Act 1986 ("POA 1986"));

(2) aggravated offences, which apply to race and religion (Crime and Disorder Act 1998 ("CDA 1998")); and

(3) enhanced sentencing, which applies to race, religion, disability, sexual orientation and transgender identity (Criminal Justice Act 2003 ("CJA 2003")).

9.16 We then look again at the communication offences found in section 127 of the Communications Act 2003 ("CA 2003") and section 1 of the Malicious Communications Act 1988 ("MCA 1988"), which are often committed in the context of online hate speech. We also consider other POA 1986 offences and harassment offences which might be aggravated by hate.

9.17 We conclude by considering the particular challenges the online environment creates for the prosecution of hate crime offences. We illustrate these by way of hypothetical examples.

STIRRING UP HATRED OFFENCES UNDER THE POA 1986

9.18 The offences of stirring up racial hatred were introduced by the POA 1986 when it was first enacted to combat certain forms of threatening, abusive or insulting conduct that are intended or likely to stir up racial hatred.[15] Similar offences covering religious hatred and hatred on the grounds of sexual orientation were added to the POA 1986 more

---

13 Equality and Human Rights Commission, *Causes and motivations of hate crime* (2016) pp 45 to 48.

14 MA Walters, *Hate Crime and Restorative Justice: Exploring Causes; Repairing Harms* (2014) p 9.

15 Public Order Act 1986, ss 18 to 23.

recently, taking effect from 2007 and 2010 respectively.[16] However, these latter offences are considerably narrower in scope, as we outline further below.

9.19 The prosecution of stirring up offences requires the consent of the Attorney General, and the maximum penalty for all these offences is seven years' imprisonment, or an unlimited fine, or both.[17]

9.20 The number of prosecutions for "stirring up" offences is very low; there were only nine prosecutions in the financial year from 2017 to 18, and this was the highest number of prosecutions since the CPS began reporting on hatred.[18] The CPS cites the high evidential threshold of the offences and the need to consider the right to freedom of expression in making prosecutorial decisions as reasons for the low numbers.[19] As we note below, the availability of communication offences which are easier to prosecute and other POA 1986 offences, is also likely to be a contributing factor.

Elements of the offences

Stirring up racial hatred

9.21 The offences based on stirring up racial hatred apply where a person engages in certain forms of threatening, abusive or insulting conduct and either:

(1) their intention was to stir up racial hatred; or

(2) having regard to all the circumstances, racial hatred was likely to be stirred up thereby.[20]

9.22 The offences do not criminalise conduct expressing hatred towards specific individuals. Rather, they address conduct intended or likely to cause others to hate "a group of persons… defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins."[21]

9.23 The term "hatred" is not defined further in the POA 1986, but it is clear that stirring up hatred is a high threshold; and goes beyond stirring up mere ridicule, or dislike or causing offence.[22]

---

16 The hate crime offences on the grounds of religion were added by the Racial and Religious Hatred Act 2006 and the sexual orientation offences by the Criminal Justice and Immigration Act 2008. They were commenced in October 2007 (SI 2007 No 2490) and March 2010 (SI 2010 No 712) respectively.

17 Public Order Act 1986, ss 27, 29L.

18 Crown Prosecution Service, *Hate Crime Report 2017-18* (October 2018) p 13, available at https://www.cps.gov.uk/sites/default/files/documents/publications/cps-hate-crime-report-2018.pdf.

19 Crown Prosecution Service, *Hate Crime Report 2017-18* (October 2018) p 12, available at https://www.cps.gov.uk/sites/default/files/documents/publications/cps-hate-crime-report-2018.pdf.

20 Public Order Act 1986, s 17.

21 Public Order Act 1986, s 17.

22 CPS Prosecution guidance in relation to stirring up hatred on the grounds of sexual orientation described the threshold of hatred as follows: "conduct or material which only stirs up ridicule or dislike, or which simply causes offence, would not meet the requisite threshold required by the Act, ie hatred. So, for example, the offences do not, and are not intended to extend per se to childish name calling, or the telling of jokes, or the

9.24 The stirring up offences are conduct crimes. They do not require proof that hatred has in fact been stirred up, merely that it was either intended or likely. However, where the fault element of intention is not proved, and the prosecution is seeking to demonstrate the alternative – that racial hatred was "likely to be stirred up" – the legislation states that the offence is not committed if the defendant "did not intend his words or behaviour, or the written material, to be, and was not aware that it might be, threatening, abusive or insulting".[23]

9.25 Short of proving intention to stir up racial hatred, therefore, a defendant can only be found guilty of a stirring up offence if:

(1) the defendant used or displayed threatening, abusive or insulting words, behaviour or written material;

(2) the defendant intended the words, behaviour or written material to be threatening, abusive or insulting or was aware that they might be threatening, abusive or insulting; and

(3) having regard to all the circumstances, racial hatred was likely to be stirred up thereby.

9.26 The six types of conduct caught by the stirring up of racial hatred offences are:

(1) using threatening, abusive or insulting words or behaviour or displaying written material which is threatening, abusive or insulting;

(2) publishing or distributing written material which is threatening, abusive or insulting;

(3) presenting or directing the public performance of a play involving the use of threatening, abusive or insulting words or behaviour;

(4) distributing, showing or playing a recording of visual images or sounds which are threatening, abusive or insulting;

(5) providing a programme service, or producing or directing a programme, where the programme involves threatening, abusive or insulting visual images or sounds, or using the offending words or behaviour therein; and

(6) possessing written material, or a recording of visual images or sounds, which is threatening, abusive or insulting, with a view to it being displayed, published, distributed, shown, played or included in a cable programme service.[24]

---

preaching of religious doctrine, unless those activities are threatening or intended to stir up hatred". See Crown Prosecution Service, *Homophobic, Biophobic and Transphobic Hate Crime – Prosecution Guidance* (15 August 2018), available at https://www.cps.gov.uk/legal-guidance/homophobic-biphobic-and-transphobic-hate-crime-prosecution-guidance.

[23] Public Order Act 1986, s 18(5). In relation to religious hatred and hatred on the grounds of sexual orientation, an equivalent provision exists under section 29B(5) of the Public Order Act 1986.

[24] Public Order Act 1986, ss 18 to 23.

9.27 Almost all of this conduct could be committed online.

9.28 In *R v Sheppard*,[25] the Court of Appeal held that publication on the internet meets the requirement of the offence that publication be to the public or a section of the public if through such placement it is generally accessible or available to, placed before, or offered to the public.[26] The Court rejected the argument that there cannot be publication without a publishee, finding that this was based on an irrelevant comparison with the law of tort.[27]

9.29 Following the decision in *R v Burns*,[28] it appears clear that it is not necessary that the intended or likely target of the stirring up of hatred be located within the jurisdiction of England and Wales.

Stirring up religious hatred and hatred on the basis of sexual orientation

9.30 Similar conduct is caught by the offences relating to stirring up hatred based on religion and sexual orientation,[29] but there are some important differences which make them narrower in scope:

(1) the words or conduct must be threatening (not merely abusive or insulting);

(2) there must have been an intention to stir up hatred (a likelihood that it might be stirred up is insufficient); and

(3) there are express provisions protecting freedom of expression covering, for example, criticism of religious beliefs[30] or sexual conduct.[31]

9.31 These criteria make the offences of stirring of religious hatred and stirring up hatred on the basis of sexual orientation even more difficult to prosecute than stirring up racial hatred.

9.32 We detail the particular "freedom of expression" protections further at paragraphs 9.36 to 9.39 below.

---

25 [2010] EWCA Crim 65; [2010] 1 WLR 2779.

26 *R v Sheppard* [2010] EWCA Crim 65; [2010] 1 WLR 2779 at [34].

27 *R v Sheppard* [2010] EWCA Crim 65; [2010] 1 WLR 2779 at [35].

28 [2017] EWCA Crim 1466.

29 See Public Order Act 1986, ss 29B to 29G.

30 Public Order Act 1986, s 29J.

31 Public Order Act 1986, s 29JA.

Protected groups

Racial hatred

9.33 Racial hatred is defined for the purposes of the stirring up offences to mean hatred against a group of persons defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins.[32]

Religious hatred

9.34 Religious hatred is defined as hatred against a group of persons defined by reference to religious belief or lack of religious belief.[33]

Hatred on the grounds of sexual orientation

9.35 Hatred on the grounds of sexual orientation is defined as hatred against a group of persons defined by reference to sexual orientation, whether towards persons of the same sex, the opposite sex or both.[34] It does not extend to other forms of sexual preference that are not related to gender.

Protection of freedom of expression

9.36 The POA 1986 sets out fairly broad protections for freedom of expression in respect of religion and sexual conduct or practice, but not racial hatred.

9.37 In relation to religion, the POA 1986 states:

> Nothing in this Part shall be read or given effect in a way which prohibits or restricts discussion, criticism or expressions of antipathy, dislike, ridicule, insult or abuse of particular religions or the beliefs or practices of their adherents, or of any other belief system or the beliefs or practices of its adherents, or proselytising or urging adherents of a different religion or belief system to cease practising their religion or belief system.[35]

9.38 Similarly, in relation to sexual orientation, protection is provided for:

(1) the discussion or criticism of sexual conduct or practices or the urging of persons to refrain from or modify such conduct or practices; and

(2) discussion or criticism of marriage which concerns the sex of the parties to marriage.[36]

9.39 The distinction between religious belief and race can be significant for ethno-religious groups, where there is a blurring of boundaries between religion and ethnicity. For

---

32 Public Order Act 1986, s 17.

33 Public Order Act 1986, s 29A.

34 Public Order Act 1986, s 29B.

35 Public Order Act 1986, s 29J.

36 Public Order Act 1986, s 29JA.

example, Sikhs[37] and Jews[38] have been held in non-criminal contexts to be members of a racial group as well as a religious group.

Stirring up offences where material hosted overseas

9.40 The Court of Appeal has held that the use of a foreign web server to upload content prepared in England and Wales, and intended for a domestic audience, gives the courts of England and Wales jurisdiction. In *Sheppard*,[39] the defendants resided and operated in England but published racially inflammatory material on a website hosted in California. They were convicted of stirring up racial hatred contrary to the POA 1986, and one of their grounds of appeal was that the case could only be tried in the jurisdiction where the web server was located.

9.41 In rejecting this ground of appeal, the Court noted that material complained of was prepared in England and Wales, was uploaded onto the website from England and Wales, and that this must have been done in the knowledge and with the expectation and intent that the material should be available to the public or a section of it within England and Wales.[40] However, as we have noted in Chapter 2, the legal position is less clear in respect of material both created and published outside the jurisdiction but intended for an audience in England and Wales.

RACIALLY AND RELIGIOUSLY AGGRAVATED OFFENCES

9.42 The CDA 1998 creates a number of separate racially or religiously aggravated versions of offences that already exist in the criminal law.[41] These aggravated versions of the offences have higher maximum sentences. The offences which have racially and religiously aggravated versions are:

(1) malicious wounding or inflicting grievous bodily harm contrary to section 20 of the Offences Against the Person Act 1861;

(2) assault occasioning actual bodily harm contrary to section 47 of the Offences Against the Person Act 1861;

(3) common assault;

(4) destroying or damaging property contrary to section 1(1) of the Criminal Damage Act 1971;

(5) threatening, abusive or insulting conduct intended, or likely, to provoke violence or cause fear of violence contrary to section 4 of the POA 1986;

---

37 *Mandla v Dowell-Lee* [1983] 2 AC 548.

38 *R (on the application of E) v JFS Governing Body* [2009] UKSC 15; [2010] 2 AC 728.

39 *R v Sheppard* [2010] EWCA Crim 65; 1 WLR 2779.

40 *R v Sheppard* [2010] EWCA Crim 65; 1 WLR 2779 at [22].

41 Aggravated offences were first introduced in respect of racial hostility by the Crime and Disorder Act 1998, ss 28 to 32. Religiously aggravated offences were subsequently added by the Anti-terrorism, Crime and Security Act 2001, s 39.

(6) threatening, abusive or insulting conduct intentionally causing harassment, alarm or distress contrary to section 4A of the POA 1986;

(7) threatening or abusive conduct likely to cause harassment, alarm or distress contrary to section 5 of the POA 1986;

(8) harassment and stalking contrary to sections 2 and 2A of the Protection from Harassment Act 1997 ("PHA 1997"); and

(9) putting people in fear of violence, and stalking involving fear of violence, serious alarm or distress contrary to sections 4 and 4A of the PHA 1997.[42]

9.43 We consider a number of these offences – notably those under the POA 1986 and PHA 1997 – in more detail in other Chapters that address threats (Chapter 7) and harassment and stalking (Chapter 8).

9.44 These offences are not a comprehensive list of the types of offences that are committed in the context of hate crime; for example, sexual offences and the communication offences under section 127 of the CA 2003 and section 1 of the MCA 1988 are not covered.[43] In cases in which hate offending occurs in the commission of those offences, the prosecutor must have recourse to the CJA 2003 enhanced sentencing regime that we outline later in this Chapter.

Meaning of "racial group"

9.45 Racial group is defined as "a group of persons defined by reference to race, colour, nationality (including citizenship) or ethnic or national origins".[44]

9.46 Racial terms are considered within the factual context in which they are used, and terms such as "immigrant"[45] and "foreigner"[46] are capable of falling within the definition of racial aggravation.

Meaning of "religious group"

9.47 Religious group is defined as "a group of persons defined by reference to religious belief or lack of religious belief".[47]

9.48 This definition allows for aggravation to be on the basis that the victim rejects religious belief, but it does not extend to hostility based on non-religious beliefs such as environmentalism.

---

42 Crime and Disorder Act 1998, ss 29 to 32.

43 C Bakalis, "Legislating against hatred: the Law Commission's report on hate crime" [2015] 3 *Criminal Law Review* 192, p 202.

44 Crime and Disorder Act 1998, s 28(4).

45 *Attorney General's Reference (No 4 of 2004)* [2005] EWCA Crim 889; [2005] 1 WLR 2810.

46 *Rogers* [2007] UKHL 8; [2007] 2 AC 62.

47 Crime and Disorder Act 1998, s 28(5).

What makes a crime racially or religiously aggravated?

9.49 An offence becomes racially or religiously aggravated if it can be proved that:

(1) at the time of committing the offence, or immediately before or after doing so, the offender demonstrates towards the victim of the offence hostility based on the victim's membership (or presumed membership) of a racial or religious group; or

(2) the offence is motivated (wholly or partly) by hostility towards members of a racial or religious group based on their membership of that group.[48]

9.50 Hostility itself is not defined in the CDA 1998. It is ultimately a question of fact for the tribunal to decide whether a defendant has "demonstrated" hostility, or been "motivated by" hostility. These concepts are outlined below.

Demonstrates hostility

9.51 The use of racially abusive insults will ordinarily be sufficient to prove demonstration of racial hostility.[49] It may also be demonstrated in other ways, such as visual symbols (for example, swastikas) or singing certain songs.[50]

9.52 Whether hostility was demonstrated is a wholly objective question. The victim's perception of, and the perpetrator's motivation for the offence is not relevant to the question of whether hostility was objectively demonstrated.[51] So, for example the fact that the defendant's frame of mind was such that, while committing the offence, he or she would have used abusive terms towards *any* person by reference to personal characteristics, has been determined not to be a defence to a finding that hostility was demonstrated.[52]

9.53 Hostility must be demonstrated either at the time of committing the offence or immediately before or immediately after doing so.[53] In *R v Babbs*,[54] the Court of Appeal found that in the context of an assault that occurred up to 15 minutes after racial hostility had been demonstrated, it was still open to the jury to find that there was a sufficient connection between the conduct and the assault and it was therefore racially aggravated.[55]

---

48 Crime and Disorder Act 1998, s 28.

49 *DPP v Pal* [2000] *Criminal Law Review* 756.

50 *R v Rogers* [2007] UKHL 8; [2007] 2 AC 62 at [13].

51 *DPP v Green* [2004] EWHC 1225 (QB); *The Times* 7 July 2004.

52 *Woods* [2002] EWHC 85 (Admin) at [13]. See also Crime and Disorder Act 1998, s 28(3), which states that "it is immaterial… whether or not the offender's hostility is *also* based, to any extent, on any other factor".

53 Crime and Disorder Act 1998, s 28(1)(a).

54 [2007] EWCA Crim 2737.

55 *R v Babbs* [2007] EWCA Crim 2737.

Motivated by hostility

9.54 Whether a defendant is "motivated by hostility" depends on the defendant's subjective motivation. The hostility does not need to be the sole or even the main motivation for committing the offence;[56] but it must be one of the motivations.[57]

9.55 CPS guidance on racially and religiously aggravated hate crime states:

> Motive can be established by evidence relating to what the defendant may have said or done on other occasions or prior to the current incident. In some cases, background evidence could well be important if relevant to establish motive, for example, evidence of membership of, or association with, a racist group, or evidence of expressed racist views in the past might, depending on the facts, be admissible in evidence.[58]

9.56 It is generally more difficult to prove that a person was motivated by hostility than that they demonstrated hostility. Motivation requires evidence of the defendant's state of mind, not just their conduct.

HATE CRIME AND ENHANCED SENTENCING

9.57 Enhanced sentencing for mandatory aggravating factors for offences aggravated by hostility was introduced by the CJA 2003. It applies much more broadly than the aggravated offences scheme referred to above.

9.58 Section 145 of the CJA 2003 requires racial and religious hostility to be taken into account at the sentencing stage for all criminal offences other than those charged as aggravated offences (as in this case the offence itself is already aggravated). Section 146 requires the sentencing court to take into account hostility based on disability, sexual orientation, and transgender identity in sentencing for any offence.

9.59 The key differences between this regime and the aggravated offences regime under the CDA 1998 are that:

(1) the CDA 1998 allows for a higher maximum sentence for each of the offences if aggravated, whereas the CJA 2003 increases the sentence within the existing maximum for the basic offence;

(2) under the CDA 1998, the aggravation is part of the offence, and will be assessed by a jury at the liability stage, whereas under the CJA 2003 the hostility element will be determined by a judge at the sentencing stage; and

(3) a further key distinction is that the fact of the racial or religious aggravation under the CDA 1998 will appear on an offender's criminal record. While the court is obliged to state aggravation under the CJA 2003 in open court, it will not appear on the offender's criminal record. In our 2014 report, we recommended that this

---

56 *DPP v McFarlane* [2002] EWHC 485 (Admin).

57 *DPP v Howard* [2008] EWHC 608 (Admin).

58 Crown Prosecution Service, *Racist and Religious Hate Crime – Prosecution Guidance* (15 August 2018), available at https://www.cps.gov.uk/legal-guidance/racist-and-religious-hate-crime-prosecution-guidance.

discrepancy should be removed, and the use of the enhanced sentencing provisions should always be recorded on the Police National Computer (PNC) and reflected on the offender's record.[59]

Racial or religious aggravation

9.60 Section 145 of the CJA 2003 provides that when considering the seriousness of a crime (other than one under sections 29 to 32 of the CDA 1998),[60] if the court finds that the crime was racially or religiously aggravated then the court:

(1) must treat that fact as an aggravating factor; and

(2) must state in open court that the offence was so aggravated.

9.61 It cannot be used to increase a sentence where the offender was acquitted of an aggravated offence but convicted of the corresponding non-aggravated offence.[61] However, there may be circumstances where aggravation under section 145 can apply at sentencing, where the prosecution has not pursued an aggravated version of the offence.[62]

9.62 The meaning of "racially or religiously aggravated" in this context is the same as that used in the CDA 1998: that the offending demonstrated or was motivated by hostility based on race or religion.[63]

Aggravation related to disability, sexual orientation or transgender identity

9.63 Section 146 similarly states that in considering the seriousness of offending that is aggravated in relation to disability, sexual orientation or transgender identity, the court:

(1) must treat the fact that the offence was committed in any of those circumstances as an aggravating factor; and

(2) must state in open court that the offence was committed in such circumstances.[64]

9.64 Unlike section 145, section 146 does not make reference to the CDA 1998. However, it creates an almost identical scheme that aggravates the seriousness of offending where:[65]

(1) at the time of committing the offence, or immediately before or after doing so, the offender demonstrated towards the victim of the offence hostility based on:

---

59 Hate Crime: Should the Current Offences be Extended? (2014) Law Com No 348, para 3.104.

60 Bakalis has noted the "problematic coexistence" of these two regimes, particularly in respect of the mutual exclusivity provisions, see C Bakalis, "Legislating against hatred: the Law Commission's report on hate crime" [2015] 3 *Criminal Law Review* 192, p 194.

61 *R v McGillivray* [2005] EWCA Crim 604.

62 See *R v O'Leary* [2015] EWCA Crim 1306; [2016] 1 Cr App R (S) 11.

63 Criminal Justice Act 2003, s 145(3); Crime and Disorder Act 1998, s 28.

64 Criminal Justice Act 2003, s 146(3).

65 Criminal Justice Act 2003, s 146(2).

(a) the sexual orientation (or presumed sexual orientation) of the victim;

(b) a disability (or presumed disability) of the victim; or

(c) the victim being (or being presumed to be) transgender; or

(2) the offence is motivated (wholly or partly)

(a) by hostility towards persons who are of a particular sexual orientation;

(b) by hostility towards persons who have a disability or a particular disability; or

(c) by hostility towards persons who are transgender.

Evidence of hostility for the purposes of enhanced sentencing

9.65 Whereas hostility must be proved as part of the offence for the purpose of the aggravated offences under the CDA 1998, under the enhanced sentencing regime it is a question of fact for the judge.

9.66 If the offender wishes to challenge the allegation that hostility was present and that the sentence should be enhanced in accordance with section 145 or 146, the prosecution will have to provide evidence. If the defendant has pleaded guilty on a limited basis[66] (for example, they do not accept that the offending demonstrated or was motivated by hostility) then a *Newton* hearing may take place to decide on the facts that remain in dispute between the defence and the prosecution that are relevant to sentencing.[67] In a *Newton* hearing the judge acts as the tribunal of fact, applying the criminal burden and standard of proof. It will only be necessary where there is likely to be a significant impact on the sentence.[68]

Meaning of disability

9.67 Disability is defined broadly as "any physical or mental impairment".[69]

---

66 There are clear CPS guidelines on the acceptance of guilty pleas, which require that prosecutors should only accept the defendant's plea if they think the court is able to pass a sentence that matches the seriousness of the offending, particularly where there are aggravating features. See Crown Prosecution Service, *Accepting Guilty Pleas*, at para 9.2, available at https://www.cps.gov.uk/publication/accepting-guilty-pleas.

67 See *R v Newton* (1983) 77 Cr App R 13.

68 Detailed guidance is set out in *R v Underwood* [2004] EWCA Crim 2256; [2005] 1 Cr App R 13. However, the Attorney General's guidance states that "the basis of a guilty plea must not be agreed on a misleading or untrue set of facts and must take proper account of the victim's interests". See Attorney General's Office, *The Acceptance of Pleas and the Prosecutor's Role in the Sentencing Exercise* (2012), available at https://www.gov.uk/guidance/the-acceptance-of-pleas-and-the-prosecutors-role-in-the-sentencing-exercisec-the-basis-of-plea.

69 Criminal Justice Act 2003, s 146(5).

9.68 Prosecution of hate crimes on the basis of disability can present particular challenges. One of these is that not all disabilities are obvious. This can make it more difficult to show that the offender was motivated by hostility towards disability or a disabled person.

9.69 Disability hate crime can also be masked as "mate crime",[70] a phenomenon where people with learning disabilities or mental health issues are "befriended" by people who then exploit them.

9.70 There is also an important distinction between crimes that demonstrate or are motivated by hostility towards disabled people, and crimes that are opportunistically targeted towards disabled people because they are perceived to be more vulnerable as a result of their particular disability (for example, they have a physical impairment that makes it easier to steal from them without resistance/challenge). In the latter case there may be no evidence that the offender dislikes or hates the person or disabled people. Targeting of vulnerability is itself an aggravated factor in sentencing,[71] albeit a distinct one.

9.71 The CPS has developed a detailed policy on disability hate crime and other crimes against disabled people, which defines "crimes against disabled people" as:

> Any crime in which disability is a factor, including the impact on the victim and where the perpetrator's perception that the victim was disabled was a determining factor in his or her decision to offend against the specific victim.

9.72 CPS policy is "to put before the court any evidence that a disabled person is targeted for this reason, so that the sentence reflects the gravity of such offending".[72]

Meaning of sexual orientation

9.73 Sexual orientation is not further defined in the legislation, but has been interpreted to cover sexual activity between people of the same sex, the opposite sex, or both.[73]

9.74 It does not cover preferences for particular acts or practices. For example, in *R v B*[74] the Court of Appeal was clear that it did not extend to perceived paedophile activity.

---

70 For further discussion, see P Thomas, "'Mate crime': ridicule, hostility and targeted attacks against disabled people" (2011) *Disability and Society* 26(1).

71 Sentencing Guidelines Council, *Overarching Principles: Seriousness* (December 2004) p 6, available at https://www.sentencingcouncil.org.uk/wp-content/uploads/web_seriousness_guideline.pdf.

72 Crown Prosecution Service, *Hate Crime: Public statement on prosecuting disability hate crime and other crimes against disabled people* (August 2017), available at https://www.cps.gov.uk/sites/default/files/documents/publications/disability-hate-crime-public%2520statement-2017.pdf.

73 Ministry of Justice, *Offences of stirring up hatred on the grounds of sexual orientation* (Circular 2010/05, 23 March 2010), available at https://www.banksr.co.uk/images/Other%20Documents/Judicial%20material/circular-2010-05-sexual-orientation-hatred.pdf.

74 *R v B* [2013] EWCA Crim 291; [2013] 2 Cr App R (S) 69.

Meaning of transgender identity

9.75 Transgender is defined to "include references to being transsexual, or undergoing, proposing to undergo or having undergone a process or part of a process of gender reassignment".[75]

9.76 This definition is intended to be inclusive, not exhaustive.[76]

SUBSTANTIVE OFFENCES PURSUED IN THE CONTEXT OF ONLINE HATE

9.77 There are four main ways that online hate crime offending may be pursued as a substantive offence:

(1) as a "stirring up" offence under the POA 1986;

(2) as hate crime aggravated harassment under the Protection from Harassment Act 1997;

(3) as a hate crime aggravated public order offence under sections 4, 4A or 5 of the POA 1986; and

(4) as a communication offence under section 127(1) of the CA 2003, or section 1 of the MCA 1988, with sentencing enhanced due to the presence of hostility towards one of the five protected characteristics.

9.78 Whereas the first three of these categories are hate crime offences in their own right (either by their nature or by virtue of the CDA 1998), communication offences with a hate crime dimension are only subject to enhanced sentencing under the CJA 2003.

9.79 In practice, the communications offences are the most frequently charged in the context of online hatred.

Stirring up hatred offences

9.80 The most direct form of hate crime offending online is the commission of one of the stirring up offences referred to above.

9.81 The number of prosecutions for these offences is very low compared to other forms of hate crime, but there have been some important convictions. For example, following the racially aggravated murder of black teenager Anthony Walker in 2005, a man who posted a series of six racist messages on a memorial website was convicted of stirring up racial hatred, and was sentenced to two years and eight months' imprisonment.[77] In 2009, Simon Sheppard and Stephen Whittle were sentenced to four years and 10

---

75 Criminal Justice Act 2003, s 146(6).

76 In the Committee of the Whole House on the Bill for the Legal Aid, Sentencing and Punishment of Offenders Act 2012 – which inserted a new section 146(6) of the Criminal Justice Act 2003 – the Minister of State, Ministry of Justice, Lord McNally said "… I should be clear that "transgender" is an umbrella term that includes, but is not restricted to, being transsexual", see *Hansard* (HL), 7 February 2012, vol 735, col 153.

77 BBC, *Walker race hate messager jailed* (6 October 2006), available at http://news.bbc.co.uk/1/hi/england/merseyside/5412558.stm.

months', and two years and four months' imprisonment respectively for publishing a variety of racially hateful material online.[78]

9.82 In a recent report on abuse, hate and extremism online, the Home Affairs Select Committee identified numerous examples of online content intended to stir up racial and religious hatred.[79]

9.83 The Sentencing Council has recently published a consultation paper for Public Order Act offences. It suggests that hate speech that is committed by influential figures, and the widespread dissemination of hateful material through forums such as YouTube, should cause the offending to be in the highest harm category for the purposes of sentencing.[80]

Hate crime and enhanced sentencing of communications offences

9.84 Given the limited application and low number of prosecutions for "stirring up" offences, in practice the majority of online hate speech that is prosecuted is pursued as one of the communications offences. In other words, a "grossly offensive" or "menacing" communication under section 127(1) of the CA 2003, or section 1 of the MCA 1988.

9.85 In the financial year from 2017 to 18, 214 offences under section 127 of the CA 2003 and 221 offences under section 1 of the MCA 1988 were flagged by prosecutors as hate crimes. This represented approximately 7% of all communications offences prosecutions.[81]

9.86 A recent example of such a prosecution was the case of Alison Chabloz, who was convicted of three offences under the CA 2003 in relation to antisemitic songs that were uploaded onto YouTube.[82] One song was titled "(((survivors)))", a play on the online convention used by white supremacists who place Jewish names within three brackets. Lyrics to the songs included:

> Did the Holocaust ever happen? Was it just a bunch of lies? Seems that some intend to pull the wool over our eyes.
>
> Now Auschwitz, holy temple, is a theme park just for fools, the gassing zone a proven hoax, indoctrination rules.

9.87 While Chabloz defended her songs as satire, Westminster Magistrates' Court was satisfied that they were grossly offensive and intended to offend Jewish people. She

---

78 See *R v Sheppard* [2010] EWCA Crim 65; [2010] 1 WLR 2779.

79 Hate crime: abuse, hate and extremism online: Government Response to the Committee's Fourteenth Report of Session 2016 – 2017 (2017) Cm 9566.

80 Sentencing Council, *Public Order Offences Guidelines Consultation* (May 2018) pp 50 to 51, available at https://www.sentencingcouncil.org.uk/wp-content/uploads/6.4328_Public_Order_Offences_Guideleines_Consultation_web.pdf.

81 Crown Prosecution Service, *Hate Crime Report 2017-18* (October 2018) p 18, available at https://www.cps.gov.uk/sites/default/files/documents/publications/cps-hate-crime-report-2018.pdf.

82 BBC, *Alison Chabloz avoids jail over anti-Semitic songs* (14 June 2018), available at https://www.bbc.co.uk/news/uk-england-derbyshire-44484632.

was sentenced to 20 weeks' imprisonment, suspended for two years, with a social media ban and 180 hours of unpaid work.

9.88 In Chapter 5 we discuss the concept of "gross offensiveness", emphasising the difficulty in determining the threshold at which prosecutions should be pursued in online communication – including hate speech – and ensuring consistency in charging practice. For example, in the above example of Alison Chabloz, the CPS initially elected not to prosecute her conduct, but later took over the case after a private prosecution had been initiated. A court then subsequently determined that criminal conduct had indeed been committed.

Hate crime aggravated harassment offences

9.89 As we note in Chapter 8, offences under the PHA 1997 are another type of offence that may be pursued in the context of hate crime.

9.90 They are offences which can be aggravated under the CDA 1998,[83] or otherwise subject to enhanced sentencing under section 146 of the CJA 2003.

9.91 For example, in March 2018, the leader and deputy leader of the far-right political organisation "Britain First" were convicted of racially aggravated harassment (amongst other offences) following the distribution of leaflets and posting of online videos during a gang-rape trial. They were sentenced to 18 and 36 weeks' imprisonment respectively.[84]

9.92 Section 1(1A) of the PHA 1997 also specifically provides for the case of harassment by an individual targeting a group, which could include people who share a particular characteristic.

9.93 However, as Bakalis notes, the PHA 1997 offences are primarily focused on conduct directed towards a specific individual or individuals, and are less suitable in cases where hateful comments are not directed at anyone in particular.[85]

Other hate crime - aggravated Public Order Act offences

9.94 In addition to the specific offence of stirring up racial hatred, other aggravated POA 1986 offences relating to hate crime – specifically the offences of "fear or provocation of violence",[86] "intentional harassment, alarm or distress"[87] and "harassment, alarm or distress"[88] – can be pursued in an online context. We discuss the offences themselves in more detail in Chapters 7 and 8.

---

83 Crime and Disorder Act 1998, s 32.

84 BBC, *Britain First leader and deputy leader jailed for hate crimes* (7 March 2018), available at https://www.bbc.co.uk/news/uk-england-43320121.

85 C Bakalis, "Rethinking cyberhate laws" (2018) 27(1) *Information & Communications Technology Law* 86, p 92.

86 Public Order Act 1986, s 4.

87 Public Order Act 1986, s 4A.

88 Public Order Act 1986, s 5.

9.95 As we have noted above, if the offender demonstrates hostility based on, or motivated by, race or religion, their conduct may amount to an aggravated offence under the CDA 1998, and incur greater maximum penalties.[89]

9.96 For example, in 2012, a man who made a number of racially offensive tweets following the on-field collapse of footballer Fabrice Muamba (who was initially feared to have died), was charged with the racially aggravated version of the offence of fear or provocation of violence contrary to section 4A of the POA 1986. He was sentenced to 56 days' imprisonment.[90] His initial tweet was "LOL, Fuck Muamba. He's dead." Following criticism of his comment he continued to tweet highly offensive and racist statements."[91]

9.97 While there is no aggravated version of the POA 1986 offences in respect of sexual orientation, disability or transgender status, the court must treat demonstration of hostility based on these characteristics as an aggravating sentencing factor.[92]

OTHER HATE CRIME RELATED OFFENCES

9.98 There are a number of other specific offences that have a hate crime dimension, including unauthorised disclosure of information relating to a gender recognition certificate, racist chanting at football matches, and attacks in religious contexts.

9.99 The police and CPS policy is to treat unauthorised disclosures under section 22 of the Gender Recognition Act 2004 as potential hate crimes if the alleged victim or any other person perceives them as such.[93]

9.100 There are also a number of specific hate-crime related offences that have a physical dimension that means they cannot be committed online.

9.101 Section 3 of the Football (Offences) Act 1991 creates an offence of engaging or taking part in chanting of an "indecent or racialist nature at a designated football match". The maximum penalty is a fine of £1000.[94]

---

89 Crime and Disorder Act 1998, ss 28 and 31(1).

90 S Morris, *Student jailed for racist Fabrice Muamba tweets* (2 March 2012), available at https://www.theguardian.com/uk/2012/mar/27/student-jailed-fabrice-muamba-tweets. The defendant subsequently appealed the severity of the sentence – the appeal was dismissed. See *R v Liam Stacey* (30 March 2012) Swansea Crown Court (unreported).

91 S Morris, *Student jailed for racist Fabrice Muamba tweets* (2 March 2012), available at https://www.theguardian.com/uk/2012/mar/27/student-jailed-fabrice-muamba-tweets. The defendant subsequently appealed the severity of the sentence – the appeal was dismissed. See *R v Liam Stacey* (30 March 2012) Swansea Crown Court (unreported).

92 Criminal Justice Act 2003, s 146.

93 Crown Prosecution Service, *Homophobic, Biphobic and Transphobic Hate Crime - Prosecution Guidance* (15 August 2018), available at https://www.cps.gov.uk/legal-guidance/homophobic-biphobic-and-transphobic-hate-crime-prosecution-guidance.

94 Football (Offences) Act 1991, s 5(2).

9.102 Section 2 of the Ecclesiastical Courts Jurisdiction Act 1860 creates an offence of violent or indecent behaviour in any place of worship that has been certified under the Places of Worship Registration Act 1855. The maximum penalty is two months' imprisonment.

9.103 Section 36 of the Offences Against the Person Act 1861 creates an offence of assaulting "a clergyman or other minister" or preventing them from officiating at religious services. This is an either-way offence which carries a maximum penalty of two years' imprisonment.

Characteristics not specifically considered to be the subject of hate crimes

9.104 While hate crime laws currently protect only five personal characteristics, there are other characteristics that are protected by other areas of the law. For example, there are nine protected characteristics under the Equality Act 2010.[95]

9.105 Some of the more prominent characteristics not currently protected by hate crime laws include: age, gender (other than transgender status), lawful sexual activity (other than as regards the gender of the participants), political views, pregnancy and maternal status.

9.106 There have been recent calls for misogyny[96] and crimes against older people[97] to be treated as hate crimes, and therefore punished more seriously.

9.107 Though the law does not treat crimes targeted against these groups as hate crimes, some law enforcement agencies are beginning to record crimes against particular groups as such. For example, the CPS reports annually on hate crime together with "crimes against older people".[98] Since 2016, Nottinghamshire Police has been monitoring "misogyny hate crime", which it defines as "incidents against women that are motivated by the attitude of men towards women and includes behaviour targeted at women by men simply because they are women".[99]

9.108 Online abuse that is targeted at women, because they are women, was a concern that was particularly highlighted in our stakeholders' experiences event. Participants emphasised the amount of online content that has the effect of "devaluing women or degrading them sexually" and expressed concern about "the harmful effect it has on the affected individual and on society more generally".

---

95 Equality Act 2010, s 4.

96 Particularly in the context of the Voyeurism (Offences) (No 2) Bill, currently before Parliament.

97 See Daily Express, *Theresa May vows to protect elderly from 'appalling' crimes with tougher laws* (18 September 2018), available at https://www.express.co.uk/news/politics/1019503/theresa-may-elderly-crimes-tougher-laws.

98 Defined as a person over the age of 60. Sentencing for these crimes may be aggravated on the basis of the victim's perceived vulnerability.

99 BBC, *Nottinghamshire Police records misogyny as a hate crime* (13 July 2016), available at https://www.bbc.co.uk/news/uk-england-nottinghamshire-36775398.

CHALLENGES TO PROSECUTING ONLINE HATE OFFENDING

Overall challenges

9.109 In pursuing hate crime offending that is committed online, law enforcement agencies face similar challenges to those presented by other forms of abusive and offensive online offending; notably the sheer scale of the abuse, and enforcement challenges where the perpetrator is located outside the jurisdiction, or as has taken steps to conceal their identity.

9.110 We discuss these general challenges in greater detail in Chapter 2.

Issues with the applicable hate crime laws

9.111 The terms of the hate crime laws themselves also create challenges in the context of prosecution:

- as we have noted above, the stirring up offences are difficult to prosecute, and accordingly are rarely pursued;
- there is a somewhat confusing relationship between the aggravated offences in the CDA 1998 and the enhanced sentencing regime under the CJA 2003;
- there is inconsistency in the contexts in which characteristics are protected, with different characteristics receiving different levels of protection; and
- as we have noted in Chapter 5, the communication offences that are commonly prosecuted in hate crime contexts rely on rather vague and malleable concepts such as "gross offensiveness".

9.112 These issues can lead to inconsistent and unsatisfactory outcomes for victims, and heighten the already difficult task facing law enforcement and prosecutors in pursuing these crimes.

Freedom of expression

9.113 An issue that arises squarely in the context of certain forms of expression is the boundary between legitimate political or satirical expression and hate speech.

9.114 For example, in our stakeholders' experiences event, organisations campaigning against antisemitism argued that anti-semitic hate speech is often masked in what may superficially appear to be legitimate political or historical commentary.

9.115 The right to freedom of expression under Article 10 of the European Convention on Human Rights ("ECHR") is an important consideration for law enforcement, prosecutors and courts when thinking about the criminalisation of hateful communication. However, this must be balanced against other rights, notably the prohibition on the abuse of the rights of others under Article 17, which is usually engaged in the context of hate crime, and has been used to prevent offenders from relying on Article 10 as a defence in the

context of hate crime offending.[100] This is discussed further in Chapter 2. The prohibition on discrimination in Article 14 of the ECHR is also highly relevant in this context.

Implementation issues

9.116 Law enforcement have taken steps to actively counter online hate crime; for example through the establishment of a national police hub for online hate crime, which drew upon a similar model in London.

9.117 However, a recent report by Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services was somewhat critical of the response of police forces to hate crime offending online, stating:

> We are surprised that forces haven't done more to understand the changing nature of hate crime and take online offending more seriously.[101]

9.118 The report noted that while in 2015 the Home Office introduced a requirement for police forces to record cyber-enabled hate crime offences, forces have been slow to make sure that these are recorded rigorously and routinely. In the last Home Office crime figures, it was still not possible to report on this element of crime statistics, due to the perceived unreliability of the data.[102]

Examples of prosecution challenges

9.119 Below we consider examples that illustrate some of the issues that can arise in relation to hate speech online.

When is hateful speech "grossly offensive" under the MCA 1988 or CA 2003?

9.120 As we explore in Chapter 5, it has proved difficult in practice for prosecutors and courts to draw a clear line as to when speech crosses from merely "offensive", to become "grossly offensive" and therefore merits a criminal sanction.

---

100 See, eg *Norwood v UK* (2004) App No 23131/03. The applicant in this case was a member of the British National Party, who displayed in the window of his first-floor flat a large poster that depicted the World Trade Centre Towers in flame, the words "Islam out of Britain – Protect the British People", and a symbol of a crescent and star in a prohibition sign. He was convicted of the aggravated offence under section 5 of the Public Order Act 1986 / section 31 of the Criminal and Disorder Act 1998 of displaying a message with hostility towards a racial or religious group. After losing his appeal in the High Court, he applied to the European Court of Human Rights, claiming the conviction violated his right to free of expression under Article 10 of the European Convention on Human Rights. In rejecting his application, the Court found his conduct "incompatible with the values proclaimed and guaranteed by the Convention" and therefore his conduct was contrary to Article, and could not enjoy the protection afforded by Article 10.

101 Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services, *Understanding the difference: The initial police response to hate crime* (July 2018) p 80, available at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/understanding-the-difference-the-initial-police-response-to-hate-crime.pdf.

102 Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services, *Understanding the difference: The initial police response to hate crime* (July 2018) p 79, available at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/understanding-the-difference-the-initial-police-response-to-hate-crime.pdf.

Example 1

Belinda is member of a radical lesbian feminist group that deeply resents being held in any kind of association with the trans community.

She writes a blog on lesbian and feminist issues, and her most recent post includes the following:

> Men who identify as transsexual "women" are an insidious cancer on the feminist movement and an affront to all womanhood. We should do everything we can to make their lives hell.

A transsexual rights organisation representative sees the blog and reports Belinda to the police.

Analysis

9.121 Unlike the categories of race, religion and sexual orientation, there is no offence of stirring up hatred based on transgender status, so such a charge would not be open to pursue.

9.122 If a prosecution were to be considered, it is most likely that it would be as a "menacing" or "grossly offensive" communication under section 127(1) of the CA 2003 (discussed in Chapter 5).

9.123 CPS guidance states that prosecution should only be pursued if the communication is *more than* offensive, shocking or disturbing. While a reasonable person would probably find Belinda's words offensive, it is not clear that she has crossed the threshold into "grossly offensive" communication in this instance.

9.124 In defending her conduct, Belinda may also seek to rely on her right to freedom of expression under Article 10 of the ECHR, and argue that her tweet was legitimate political comment in relation to an issue that she and others perceive to be a genuine social harm. Against this, prosecutors may highlight that Article 17 of the ECHR prohibits the reliance on the ECHR as justification for the destruction of the rights of others; in this case transsexual women.

Some speech which is criminalised online is not an offence offline

9.125 As we have seen in other contexts, the language of the CA 2003 and MCA 1988 is such that communication that amounts to a criminal offence online may not be an offence if the same communication is made offline.

Example 2

After receiving criticism for her views, Belinda makes a speech to her supporters at a private event, where she makes the following further comment:

> "I was wrong to suggest that the NHS should withdraw treatment for trans women. There are some forms of treatment that are clearly appropriate. Euthanasia, for example."

Analysis

9.126 Here the speech is more likely to be found to be of a "menacing" or "grossly offensive" character.

9.127 However, as it was a communicated orally, the offences under the CA 2003 and MCA 1988 are not available. Instead there would need to be consideration of POA 1986 offences.

9.128 As noted above, there is no "stirring up" offence available in relation to transphobia.

9.129 It is also not a "threat to kill" contrary to section 16 of the Offences Against the Person Act 1861, as there is no indication in Belinda's statement that she intends to kill anyone.

9.130 Further, the offences under sections 4, 4A and 5 of the POA 1986 (which we discuss in greater detail in Chapter 7), would be unlikely to apply, as Belinda is speaking to a sympathetic audience who are unlikely to directly fear violence or feel threatened, alarmed or distressed as a result of her conduct.

9.131 This example therefore demonstrates that there are contexts where hate speech may be an offence in an online context, but no offence would be committed if the same words were used in person.

Hate speech directed at women is not a recognised category of hate crime

9.132 Misogynistic abuse is one of the most common forms of abuse that is experienced online. At present it is not specified as a particular category of abuse warranting an aggravated sentence.

Example 3

Abigail is a prominent campaigner against sexual harassment, and vocal supporter of the Me Too movement. She uses the Twitter handle @justice4womyn.

She regularly receives criticism on Twitter from opponents of her activities, but following a series of tweets detailing her personal experience of sexual assault, she is particularly horrified by the following tweet by Blair, a men's rights campaigner, which states:

> @justice4womyn you were clearly asking for it! slut

She reports the matter to the police, and the CPS pursue the case as an offence under section 127(1) of the CA 2003.

Analysis

9.133 There is a strong argument here that Blair has sent a "menacing" or "grossly offensive" communication and could therefore have committed an offence under section 1 of the MCA 1988 or section 127 of the CA 2003.

9.134 Additionally, Abigail believes Blair's conduct demonstrates clear hostility to women, and this should be explicitly stated and lead to an aggravation in the sentence Blair receives.

9.135 However, at present, hatred towards women is not one of the categories that is protected by sections 145 and 146 of the CJA 2003. This crime would therefore not be categorised as a hate crime, and sentencing of Blair would not necessarily be aggravated as such. However, it is important to note that the sentencing judge has discretion to so aggravate the sentence.

CONCLUSION

9.136 For all its positive aspects, the online environment provides a fertile environment for the dissemination of hateful content.

9.137 While prosecution levels for the "stirring up" of hatred offences are low, data provided by the CPS suggests that a not insignificant proportion of online communication prosecutions are also flagged as hate crimes.

9.138 However, the clear view expressed by participants at our stakeholders' experiences event was that far too much damaging and hateful online abuse is still being left unchallenged.

9.139 We have previously noted that in the absence of a wider review of hate crime law, there is a principled argument that the aggravated offences regime should apply consistently to all five of the currently recognised categories of hate crime.[103]

9.140 In the context of this Report, we note that gender-based online hate crime, particularly misogynistic abuse, is a particularly prevalent and damaging concern. One possible avenue to address this would be through the widening of hate crime laws to include hate crimes related to gender.

9.141 Now that the Government has announced that we are tasked with undertaking a wider review of hate crime laws, there will be an opportunity to consider these issues more thoroughly.

9.142 With regard to the specific offences of stirring up hatred, the extremely low prosecution numbers suggest that these offences are of limited utility in practice.[104] One potential conclusion that could be drawn from this is that consideration should be given to whether there is a need to lower the fault threshold necessary to establish the offences.

9.143 However, this also raises a broader issue about whether the particular nature of hate speech is adequately captured in the current criminal law. In this Chapter and in Chapter 5 we have noted that the majority of online hate speech is in practice prosecuted within the broader category of "grossly offensive" or "menacing" communications under section 1 of the MCA 1988 and section 127(1) of the CA 2003. We also noted in Chapter 5 that this term is highly malleable, and has proved challenging for prosecutors and courts to apply consistently.

9.144 As Bakalis and others have argued, the use of the term "grossly offensive" in the context of hate speech is rather antiquated, and fails adequately to capture the full extent of the damage it inflicts.[105]

9.145 Further, while sections 145 and 146 of the CJA 2003 require the court to state that an offence (such as a communications offence) is hate-aggravated where this is proven, this is qualitatively different from the offence itself being described as one of hatred, as is the case with the CDA 1998.

9.146 An issue that we consider worthy of further consideration – either in the second phase of this project, or in the context of the hate crime review – is whether the law should more explicitly address hateful communications, and label and criminalise them as such.

---

103 Hate Crime: Should the Current Offences be Extended? (2014) Law Com No 348, p 150.

104 In our recent report we argued that while there was no principled reason why the stirring up offences should not be extended to cover stirring up disability hate crime and stirring up transphobia, we did not consider that there was a sound practical justification for doing so (given the low prosecution rates of the existing stirring up offences, the practical difficulties they presented, and the existence of other offences to criminalise the conduct). See Hate Crime: Should the Current Offences be Extended? (2014) Law Com No 348, p 14.

105 C Bakalis, "Rethinking cyberhate laws" (2018) 27(1) *Information & Communications Technology Law* 86, p 99.

Chapter 10: Privacy offending and disclosure without consent

INTRODUCTION

10.1 In this Chapter, we consider the key privacy and sexual imagery-based offences that might be committed in an online context in England and Wales.

10.2 Lord Hoffmann noted in *Campbell v Mirror Group Newspapers Ltd*[1] that the notion of privacy, as the basis for the tort of breach of privacy, stems from:

> the protection of human autonomy and dignity – the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people.[2]

10.3 The right to respect for private and family life is protected by the European Convention on Human Rights ("ECHR"),[3] while the Charter of Fundamental Rights of the European Union also specifically enshrines the right to protection of personal data.[4] The latter is an area subject to comprehensive EU law, now in the form of the EU General Data Protection Regulation ("GDPR"), which was recently given effect domestically in the Data Protection Act 2018.

10.4 Equally, as we have noted elsewhere in this Report, the right to freedom of expression under Article 10 of the ECHR protects the "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers".

10.5 Inevitably, the right to personal privacy and the right to freedom of expression come into conflict at times.[5] This was illustrated recently in the case brought by Sir Cliff Richard against the BBC, following pre-charge reporting of police activity in relation to him (which never resulted in charges).[6]

10.6 Despite the human rights protections and the extensive regulatory regime that exists in respect of privacy, there has been a reluctance to impose serious criminal sanctions on individuals for privacy-related offending, other than in sexual contexts. This reflects a

---

1 [2004] UKHL 22; [2004] 2 AC 457.

2 *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22; [2004] 2 AC 457 at [51].

3 European Convention on Human Rights, art 8.

4 EU Charter of Fundamental Rights, art 8.

5 For further discussion of balancing the right to privacy with the right to freedom of expression, see, eg: S O'Leary, "Balancing rights in a digital age" (2018) 59 *Irish Jurist* 59.

6 *Richard v BBC* [2018] EWHC 1837 (Ch); *The Times* 23 July 2018 (Ch D).

similar reluctance to allow civil causes of action for breaches of privacy, although the courts have now definitively recognised a tort of misuse of private information.[7]

10.7 At the same time, the growth in the online environment – from 44 million users worldwide in 1995 to 413 million in 2000 and 3.4 billion in 2016 – has facilitated a massive increase in the exchange of personal data.[8] The level of personal detail published online and the degree of its spread have grown exponentially following the rise of social media over the past two decades. While much of this exchange is consensual and positive, breaches of personal privacy can also have devastating consequences for individuals. This can be particularly so for privacy breaches relating to sexual activity. This was evidenced in 2010, when a young man in the US – Tyler Clementi – committed suicide after footage of him kissing another man was recorded, and details of the recording were posted on Twitter.[9]

10.8 While a wide range of privacy-based offending can occur online, two common and potentially harmful forms are "doxing" (the publication of a person's private or identifiable information online), and "revenge porn" (the disclosure of private sexual images without consent, with intent to cause the victim distress).[10]

10.9 In this Chapter we begin by considering the general privacy offence of disclosing personal data without consent, contrary to section 170 of the Data Protection Act 2018 (which recently replaced a similar offence under section 55 of the Data Protection Act 1998). This offence carries a maximum penalty of a fine only.[11]

10.10 We then consider a number of further offences that involve disclosure without consent, which have both a breach of privacy and a sexual dimension:

(1) the offence of publishing the name of a complainant of certain sexual offences, contrary to section 1 of the Sexual Offences (Amendment) Act 1992;

(2) the relatively recently introduced offence of disclosing private sexual photographs and films with intent to cause distress, contrary to section 33 of the Criminal Justice and Courts Act 2015; and

(3) the offence of voyeurism contrary to section 67 of the Sexual Offences Act 2003, which includes discussion of the proposed further "upskirting" offence in the Voyeurism (Offences) (No. 2) Bill.

10.11 Each of these three offences criminalises conduct involving deliberate infringements of autonomy. However, they are each underpinned by different motivations and variously exemplify either privacy offending or sexual offending, and sometimes both. The

---

7 *Vidal-Hall v Google Inc* [2014] EWHC 13 (QB); [2014] 1 WLR 4155.

8 See J Murphy and M Roser, *Internet* (2018), available at https://ourworldindata.org/internet.

9 I Parker, *The Story of a Suicide* (6 February 2012), available at https://www.newyorker.com/magazine/2012/02/06/the-story-of-a-suicide.

10 Revenge is not always a motivation for such sharing, and the relevant offence is discussed and described below as an offence pertaining to the sharing of private sexual imagery.

11 Data Protection Act 2018, s 196(2).

offence of publishing the name of a complainant of a sexual offence is primarily a privacy-related offence (albeit in a sexual offence context), while the sharing of private sexual imagery and voyeurism offences are often perceived by victims as a form of sexual abuse,[12] as well as a serious breach of their privacy.

10.12 We conclude the Chapter with a series of examples that illustrate the issues that arise in prosecuting privacy and image-based sexual offending when committed online.

OBTAINING AND DISCLOSING PERSONAL DATA WITHOUT CONSENT

10.13 The broadest privacy offences currently in force are the offences under section 170(1) of the Data Protection Act 2018 ("DPA 2018"). These offences arise where someone has knowingly or recklessly—

(1) obtained or disclosed personal data without the consent of the controller;

(2) procured the disclosure of personal data to another person without the consent of the controller; or

(3) after obtaining personal data, retained it without the consent of the person who was the controller in relation to the personal data when it was obtained.

10.14 It is also an offence under section 171 of the DPA 2018 for a person "knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data".

10.15 For the purposes of sections 171 and 172, section 171(2)(a) defines de-identified data as data that "has been possessed in such a manner that it can no longer be attributed, without more, to a specific data subject" and section 171(b) defines data as being re-identified if "the person takes steps which result in the information no longer being de-identified within the meaning of paragraph (a)". De-identified personal data includes personal data which has had features removed which could have been used to identify a person; for example, a name, place of residence, or specific characteristics.

10.16 For example, "V"'s health information is held by her local GP under an anonymised system, whereby she is identified by a unique patient number and not her name. Someone trying to find her file will only be able to know that file is V's if they knew her unique patient number. Her file, being unable to be attributed to her, has been "de-identified" for the purposes of section 171. "D", an ex partner of V's, knows her unique patient number. D uses this to "hack" into the GP system, and obtain V's patient file. D then posts on Twitter the health data of V contained in her file, adding in V's name in the Twitter post. The post would constitute "re-identification" for the purposes of section 171 of the DPA 2018.

---

12 See L Buchan, *Over 80 Labour MPs urge Theresa May to offer anonymity to revenge porn victims* (7 July 2018), available at https://www.independent.co.uk/news/uk/politics/revenge-porn-victims-anonymity-labour-urge-theresa-may-law-change-maria-miller-richard-burgon-dawn-a8434451.html; and C McGlynn and E Rackley, "Image-Based Sexual Abuse" (2017) 37(3) *Oxford Journal of Legal Studies* 534.

10.17 "Personal data" is defined in the DPA 2018 as "any information relating to an identified or identifiable living individual".[13] The Explanatory Notes to the Act state that this is the same definition as that under the GDPR, and personal data includes a person's name, identification number, location data, an "online identifier" or "one or two factors specific to the physical, physiological, genetic, economic, cultural or social identity of that natural person".[14] A person's IP address was found to be "personal data" by the Court of Justice of the European Union because the defendant, a website, was able to attribute it to a particular person.[15]

10.18 The definition of "controller" for the purposes of the DPA 2018[16] is the same as is used in Article 4(7) of the GDPR, which states that:

> "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data …

10.19 In practice, this means the person or organisation that controls the data by determining how personal data are processed and for what purposes.

10.20 This is distinct from a "processor", defined in Article 4(8) of the GDPR as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". A processor may use their technical knowledge to carry out certain activities on the data controller's behalf, but cannot take any of the core decisions in relation to the data, such as the content of the data and what it will be used for.

10.21 These concepts have been a source of contention in an online context. Social media platforms, such as Facebook, have been determined by the EU and domestic courts to be "controllers" responsible for processing the personal data of its users and those visiting pages hosted on it, for the purposes of the data protection laws.[17] However, challenges have arisen where, for example, organisations host groups such as a "fan page" on the social media platform. In one case, the Court of Justice of the European Union considered whether they may be joint controllers and therefore have obligations

---

13 Data Protection Act 2018, s 3(2).

14 Data Protection Act 2018, Explanatory Notes at [71].

15 Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECR I.

16 Data Protection Act 2018, s 6.

17 This was reported to be "common ground" in Case C-210/16 *Unabhangiges Landeszentrum fur Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein* [2018] ECR I-388 (Grand Chamber decision). Facebook was held to be a data controller for the purposes of the Data Protection Act 1998 in *CG v Facebook Ireland Ltd* [2016] NICA 54; [2017] Entertainment and Media Law Reports 12 which applied the Court of Justice's decision in Case C-131/12 *Google Spain v AEPD and Gonzalez* [2014] ECR I-317 (Grand Chamber decision); [2014] QB 1022 and C-230/14 *Weltimmo v Nemzeti Adatvedelmi es Informacioszabadsag Hatosag* [2015] ECR I-639; [2016] 1 WLR 863.

under the GDPR and DPA 2018. It was held that the German administrator of a fan page on Facebook was jointly responsible as a controller with Facebook Ireland.[18]

10.22 The notion of "consent" and type of consent, which is not specified in the DPA 2018, can raise similar issues to that discussed below in relation to sharing private sexual images without consent. For example, if someone posts their information on to social media, an issue may arise as to whether they are consenting to further disclosure of that data.[19] It is likely that the requirement of "explicit" consent in Article 6 of the GDPR would mean that posting is not automatic consent for re-posting. However, this demonstrates that online communication can complicate such concepts without clear definition and guidance.

10.23 The maximum penalty available for these offences is a fine,[20] and prosecution can only be conducted by the Information Commissioner, or by or with consent of the Director of Public Prosecutions.[21] In practice, a Crown Prosecution Service ("CPS") lawyer will most likely prosecute the case.

10.24 While only recently introduced, the section 170(1) offences replaced similar offences that already existed under section 55 of the Data Protection Act 1998 ("DPA 1998", now repealed), together with an offence of selling such data,[22] and a new re-identification offence under section 171.

10.25 There are a number of defences available to a defendant under the DPA 2018. These are that:

- the action was necessary for the purposes of preventing or detecting crime;
- the action was required or authorised by an enactment, rule of law or court order;
- the action was justified in the public interest;
- the defendant held the reasonable belief that their action was lawful or that the controller would have consented, had they known what has happening; and
- the defendant acted with a view to the publication by a person of any journalistic, academic, artistic or literary material, and in the reasonable belief that in the particular circumstances the action was justified as being in the public interest.[23]

10.26 The offences can be committed online. For example, in February 2018, the Information Commissioner's Office ("ICO") successfully prosecuted a local authority education

---

18 Case C-210/16 *Unabhangiges Landeszentrum fur Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein* [2018] ECR I-388 (Grand Chamber decision).

19 For further discussion, see R Massey, "'A thorough analysis' of the notion of consent in the General Data Protection Regulation" (2018) 29(4) *Entertainment Law Review* 106.

20 Data Protection Act 1997, s 196(2).

21 Data Protection Act 1997, s 197(1).

22 Data Protection Act 1997, s 170(5).

23 Data Protection Act 1997, ss 170(2) and (3), and 171(3) and (4).

worker, who took a screenshot of a council spreadsheet concerning children and their eligibility for free school meals, before sending it to the estranged parent of one of the pupils via Snapchat. She was fined £850 and was also ordered to pay £713 in costs.[24]

10.27 However, given that the maximum penalty available under section 170 of the DPA 2018 is a fine, in serious "doxing" cases it is likely that the prosecutors will seek to charge a more serious offence. Doxing might, for example, form part of a broader course of conduct for the purposes of a harassment or stalking offence under the Protection from Harassment Act 1997.[25] It could also amount to one of the communications offences we discuss in Chapter 4 if the communication is found to be "menacing", "grossly offensive", "indecent" or "false". However, these offences do not cover all circumstances where someone's privacy is breached online, meaning that in some cases section 170 of the DPA 2018 will be the appropriate charge.

10.28 A significant criticism expressed at our first academic roundtable was the lack of gravity attributed to privacy offences, compared with other forms of offending. Indeed, the ICO has called for custodial sentences to be available in cases of serious misuses of personal data.[26] Under the previous DPA 1998, the Justice Secretary had been given the power to increase the sentence for the pre-existing offence,[27] but this was never done, and the power was repealed and not replaced in the DPA 2018.[28]

10.29 In our separate paper on Protection of Official Data, we similarly noted concerns that the maximum penalty for this offence is a fine, particularly given the harm that can be committed by such offences in a digital context.[29]

Other unauthorised publication offences

10.30 While the offence contrary to section 170 of the DPA 2018 is a broad, catch-all offence in relation to protection of personal data, there are also a range of offences of unauthorised disclosure of personal data that exist across various statues. These often penalise people in particular positions of authority and carry more substantial maximum penalties. Examples include:

(1) section 123 of the Social Security Administration Act 1992, which prohibits disclosure of information obtained by a person employed in social security

---

24 Information Commissioner's Office, *Samira Bouzkraoui* (2 February 2018), available at https://ico.org.uk/action-weve-taken/enforcement/samira-bouzkraoui/.

25 We discuss harassment and stalking further in Chapter 8.

26 See Information Commissioner's Office, *Information Commissioner repeats call for stronger sentences for data thieves* (11 January 2016), available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/01/information-commissioner-repeats-call-for-stronger-sentences-for-data-thieves/; and Information Commissioner's Office, *The Information Commissioner's response to the new data security standards and opt-out models for health and social care* (2016), available at https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1625007/ndg-review-consultation-ico-response-20160907pdf.pdf.

27 Section 77 of the Criminal Justice and Immigration Act 2008 gave the Secretary of State the power to increase the maximum sentence for the offences under section 55 of the Data Protection Act 1998.

28 Data Protection Act 2018, s 212(1); sch 19, para 150(a).

29 Protection of Official Data (2017) Law Commission Consultation Paper No 230, para 4.74.

administration or adjudication relating to a particular person, and is punishable by up to two years' imprisonment;

(2) sections 9 and 9A of the Rehabilitation of Offenders Act 1974, which prohibit unauthorised disclosure of spent convictions and cautions, and are punishable by up to six months' imprisonment; and

(3) section 19 of the Commissioners for Revenue and Customs Act 2005, which prohibits wrongful disclosure of revenue and customs information that is capable of identifying an individual, punishable by up to two years' imprisonment.

10.31 There are many other such offences, and we do not provide a comprehensive list in this Report. However, a common feature of all these offences is that, as a matter of law, they can all be committed in an online context.

10.32 In our Consultation Paper in relation to the Protection of Official Data we noted that there was a case to be made for a review of these various offences (we identified at least 124, but there are likely to be more), to ensure greater consistency and coherence in the law.[30]

PUBLISHING DETAILS OF A COMPLAINANT OF SEXUAL OFFENCES

10.33 In addition to the general data protection offences, there is a specific offence of publishing the details of complainants of certain sexual offences[31] which are likely to lead to their identification.[32]

10.34 The offence is one of strict liability, but it is a defence if the complainant had given written consent to the publication or programme,[33] or the person charged was not aware and neither suspected nor had reason to suspect, that the publication included the offending content.[34] Courts also have various powers to override the default position of complainant anonymity.[35]

10.35 The maximum penalty for the offence is a fine.[36]

10.36 There are limits on the protection of complainant anonymity, however. The Court of Appeal has found that it does not extend to provide a power to order that the defendant

---

30 Protection of Official Data (2017) Law Commission Consultation Paper No 230, paras 4.54 and 4.58.

31 Specified in the Sexual Offences (Amendment) Act 1992, s 2.

32 Sexual Offences (Amendment) Act 1992, s 1. Such details of complaints can include, in particular, the person's name, the person's address, the identity of any school or other educational establishment attended by the person, the identity of any place of work, and any still or moving picture of the person: see section 1(3A).

33 Sexual Offences (Amendment) Act 1992, s 5(2). But not if it is proved that any person interfered unreasonably with the peace or comfort of the person giving the consent, with intent to obtain it: see section 5(3).

34 Sexual Offences (Amendment) Act 1992, s 5(5).

35 Sexual Offences (Amendment) Act 1992, s 3.

36 Sexual Offences (Amendment) Act 1992, s 5(1).

should also be given anonymity, even when the purpose of such an order is to protect the anonymity of the complainant.[37]

10.37 The offence has been challenged on human rights grounds, and found to be consistent with the right to freedom of expression under Article 10 of the ECHR.[38]

10.38 Prosecution for this offence requires the consent of the Attorney General.[39]

10.39 Social media has now provided a platform through which the names of complainants can be published, and action has been taken in some cases. For example, in connection with the case of *Evans*, a sexual assault case involving a high-profile footballer, nine people pleaded guilty in the magistrates' court in November 2012 to publishing details likely to lead to the identification of the complainant.[40] They were ordered to pay £624 each in compensation. The harm to the complainant was significant, and the abuse she suffered led to her having to change her identity. However, the criminal sanctions imposed were not necessarily an effective deterrent; at least two other people continued to name the complainant in online blogs throughout the re-trial.[41]

10.40 In an online context, prosecuting this offence may be challenging where publication of the offending identifying material occurs outside of the United Kingdom,[42] but is accessible online within the United Kingdom.

10.41 If, for example, a complainant's name was to be reported in the United States, and this material was readily accessible in the United Kingdom, it may meet the substantial measure test outlined in *R v Sheppard*[43] such that the publisher could be committing an offence under the law of the United Kingdom. However, in practice, it would be likely to prove extremely difficult for the offence to be enforced, as extradition is usually not possible for summary offences punishable with a fine only,[44] and a prosecution would probably not be found to be in the public interest.

---

37 *R (Press Association) v Cambridge Crown Court* [2012] EWCA Crim 2434; [2013] 1 WLR 1979 [17].

38 *O'Riordan v DPP* [2005] EWHC 1240 (Admin); *The Times* 31 May 2005.

39 Sexual Offences (Amendment) Act 1992, s 4.

40 S Morris, Social media naming of Ched Evans's accuser raises legal questions (14 October 2016), available at https://www.theguardian.com/law/2016/oct/14/social-media-naming-of-ched-evans-accuser-raises-questions-l; https://www.bbc.co.uk/news/uk-wales-north-east-wales-20207408.

41 S Morris, *Social media naming of Ched Evans's accuser raises legal questions* (14 October 2016), available at https://www.theguardian.com/law/2016/oct/14/social-media-naming-of-ched-evans-accuser-raises-questions-law.

42 The Act applies to England, Wales, Scotland and Northern Ireland: Sexual Offences (Amendment) Act 1992, s 8(6).

43 [2010] EWCA Crim 65; [2010] 1 WLR 2779.

44 See Extradition Act 2003, s 148.

SHARING PRIVATE SEXUAL IMAGERY

10.42 One area where the arrival of the internet and portable internet enabled devices has led to particularly devastating consequences is in the disclosure of private sexual imagery without consent.

10.43 Websites have been created which are dedicated to this abuse, which have led to a proliferation in the distribution and consumption of such material.[45] Frequently, private sexual imagery is shared whilst other forms of domestic abuse are also occurring,[46] which illustrates how easily offline and online abuse can converge in practice.[47]

10.44 A survey by the Cyber Civil Rights Initiative ("CCRI") in 2013, and an evaluation of the Revenge Porn Helpline by Bond and Dogaru in 2015, showed that 93% of victims of this abuse had suffered significant emotional consequences, and research has documented the psychological impact of such acts.[48] In some cases, it has reportedly led to suicide.[49]

10.45 While offences such as section 127 of the Communications Act 2003 ("CA 2003") (sending an indecent message) and harassment contrary to the Protection from Harassment Act 1997, are often prosecuted in these "online" sharing scenarios, such charges are deemed by some to be insufficient from a labelling and penal perspective.[50] For example, section 127 of the CA 2003 requires the conduct to be grossly offensive, which has excluded some images that were disclosed without consent and caused distress; while harassment requires a "course of conduct" that excludes the one-off sharing of such images without consent.

10.46 In response to a growing concern about the sharing of private sexual images online, with existing legislation not designed for that purpose, the government introduced a specific offence.

---

45 S Pegg, "A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512.

46 N Henry and A Powell "Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women" (2015) 48(1) *Australian and New Zealand Journal of Criminology* 104.

47 See, eg E Bond and K Tyrell, "Understanding Revenge Pornography: A National Survey of Police Officers and Staff in England and Wales" (2018) *Journal of Interpersonal Violence*.

48 See, eg, S 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; E Bond and C Dogaru, *Evaluation of the National Revenge Pornography Helpline* (2016); and M Kamal and WJ Newman, "Revenge pornography: Mental health implications and related legislation" (2016) 44(3) *Journal of the American Academy of Psychiatry and the Law* 359.

49 See, eg the case of Damilya Jossipalenya, who took her own life after her boyfriend, Alessio Bianchi, shared sexually explicit videos and threatened to continue to do so. As of 10 June 2018, the CPS were considering manslaughter charges in the case. See G Wilford, *Man whose girlfriend committed suicide after he threatened to send revenge porn to her family may face manslaughter charges* (10 June 2018), available at https://www.thesun.co.uk/news/6495510/revenge-porn-rat-may-face-charges/.

50 For discussion of previous prosecutions under such provisions, and the background to the enactment of section 33, see S Pegg, "A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512, pp 513 to 516.

10.47 Section 33 of the Criminal Justice and Courts Act 2015 ("CJCA 2015") provides that:

> It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made:
>
> a) without the consent of an individual who appears in the photograph or films; and
>
> b) with the intention of causing that individual distress.

10.48 The offence is triable either way, with a maximum sentence of two years' imprisonment.[51]

10.49 Jason Asagba is believed to have been the first person prosecuted for the offence. Three days after it came into force, he shared private and sexual photographs of a 20-year-old woman on Facebook, and also texted images to her family.[52]

10.50 Cases like this are quite common. Data gathered by the BBC suggest there are now over 3000 reports to police of disclosing private sexual photographs or films, but cases resulting in charges are surprisingly low.[53] Internal case management information provided by the CPS shows that only 477 charges reached a first hearing at the magistrates' court in 2017.[54] A large portion of these are domestic abuse-related; the

---

51 Definitive sentencing guidelines on section 33 were published on 5 July 2018, and are effective from 1 October 2018. See Sentencing Council, *Intimidatory Offences: Definitive Guideline* (2018), pp 21 to 26, available at: https://www.sentencingcouncil.org.uk/wp-content/uploads/Intimidatory-Offences-Guideline_WEB.pdf.

52 See Crown Prosecution Service, *Prosecutors being advised to learn from revenge porn cases across the country to help them tackle this "humiliating" crime* (7 August 2015), available at http://blog.cps.gov.uk/2015/08/prosecutors-being-advised-to-learn-from-revenge-porn-cases-across-the-country-to-help-them-tackle-th.html. Asagba was given a six-month prison sentence, suspended for eighteen months, and 100 hours of unpaid work and ordered to pay costs. See BBC, *"Revenge porn" man Jason Asagba sentenced* (1 September 2015), available at https://www.bbc.co.uk/news/uk-england-berkshire-33819264.

53 BBC, *Revenge porn: One in three allegations dropped* (14 June 2018), available at https://www.bbc.co.uk/news/uk-england-44411754. The BBC estimates, from data gathered from 34 of the 43 police forces in England and Wales, that only 7% of cases resulted in charges in the 2017 to 2018 financial year. This appears to be significantly lower than in Scotland for the offence of disclosing or threating to disclose intimate photographs of films (see Abusive Behaviour and Sexual Harm (Scotland) Act 2016, s 2). See M Ellison, *Less than half revenge porn cases passed to prosecutors* (6 March 2018), available at https://www.bbc.co.uk/news/uk-scotland-42689607.

54 This is a rise from 2015 where there were only 90 charges, with 454 in 2016. From January to June 2018, 211 people were charged under section 33. Moreover, 465 prosecutions were made under section 33 of the CJCA, with 206 prosecutions in the previous year: Crown Prosecution Service, *Violence Against Women and Girls Report 2015-2016* (2016) p 19, available at https://www.cps.gov.uk/publication/cps-violence-against-women-and-girls-crime-report-2015-2016.

Note that the CPS does not collect data that constitutes official statistics as defined in the Statistics and Registration Service Act 2007. These data have been drawn from the CPS's administrative IT system, which (as with any large scale recording system) is subject to possible errors with data entry and processing.

Office for National Statistics reports that 84% of prosecutions in the year ending March 2017 were related to domestic abuse.[55]

10.51 Reflecting some of the concerns raised in our stakeholders' experiences event, a study showed that one in three allegations regarding "revenge porn" are withdrawn by complainants.[56] The reasons cited include a reluctance to participate in prosecutions, as victims are not granted anonymity as they would be for a sexual offence, and a lack of police support.[57] This was also evident in the findings of research undertaken by Huber, a doctoral candidate at Liverpool John Moores University. All activists[58] she interviewed considered a lack of anonymity to be problematic, as it proved to be a common reason for a lack of reporting. She stated:

> Victims have already been publicly shamed and embarrassed by their perpetrator and therefore, a lack of anonymity means that further attention may be drawn towards the victims and their images when cases go to court. With many of the impacts on victims being rooted in public perception resulting in increased fear of being recognised within the community, being talked about, and people viewing the images, it is negligent to assume that anonymity is not vital … Activist B clearly expressed the fundamental reason why victims needed the choice to remain anonymous:
>
> > this ordeal, they're stressed, and now you're just making it worse. Because by putting it publicly in newspapers or magazines it then feeds public perception and they feed public inquisitiveness, and [the public] start to look and it makes it 10 times worse … The public side of it is the worst bit. When it happens between you and that person before you go to court nobody is aware of it. But once it goes to court and it's in the public domain it's a whole different ball game because then you have all the comments, and the people, and the this and the that … So, they need to be allowed to have the choice, choice is really important (Activist B).

10.52 Figures also suggest that women are disproportionately affected.[59] Since the launch of the Revenge Porn Helpline in 2015, 73% of calls received have been from women and

---

55 Office for National Statistics, *Domestic abuse in England and Wales: year ending March 2017* (23 November 2017), Table 4, available at www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/domesticabuseinenglandandwales/yearendingmarch2017.

56 BBC, *Revenge porn: One in three allegations dropped* (14 June 2018), available at https://www.bbc.co.uk/news/uk-england-44411754.

57 BBC, *Revenge porn: One in three allegations dropped* (14 June 2018), available at https://www.bbc.co.uk/news/uk-england-44411754.

58 'Activist' for the purposes of Huber's research referred to anyone who had worked closely with, or supported, victims of the disclosure of private sexual imagery without consent. This included, but was not necessarily limited to, organisational workers, lawyers who specialised in these cases and also worked to raise awareness, and one activist who was a victim of disclosure of private sexual imagery without consent and became a public figure working with others who had experienced similar behaviour.

59 See, eg, A Phippen and J Agate "New social media offences under the Criminal Justice and Courts Act and Serious Crime Act: the cultural context" (2015) *Entertainment Law Review* 82. This article cited figures indicating that 90 percent of surveyed people who had experienced this form of abuse were women. However, these are not necessarily figures specific to England and Wales. The Revenge Porn Helpline also reported to the Independent that females made up 75% of calls to the organisation: S Sandhu, *Revenge*

girls.[60] In addition, 400 of the calls received have related to what is termed "sextortion":[61] where people (in some cases, criminal gangs) extract images from men by posing as women in online platforms, and then use those images to blackmail them.[62] Approximately 72% of sextortion-related calls are received from men. Historically, such calls have formed 10 to 11% of total calls. In recent months this has increased to 18 to 23% of total calls.[63] However, such acts are more likely to be prosecuted under other offences, such as blackmail, rather than section 33 of the CJCA 2015.[64]

10.53 The focus of this provision has so far been upon the breaching of the victim's privacy, although this has been the cause of debate, with some academics, stakeholder organisations and Members of Parliament calling for it to be treated as a sexual offence.[65] It has, for example, been argued that such sharing even constitutes a form of "image-based sexual abuse".[66]

10.54 As an offence that has been drafted for the online era, our conclusion that this is another offence that does apply online will be unsurprising. Social media platforms are indeed one of the common means through which these images are shared.[67] However, this is an offence which has notable limitations built in, and has been criticised by some of our victim stakeholders for its narrow limits in certain respects. These limitations are explored further below.

---

porn complaints soar after screening of Channel 4 documentary (23 August 2015), available at https://www.independent.co.uk/news/uk/crime/revenge-porn-complaints-soar-after-screening-of-channel-4-documentary-10467349.html.

60 Figures disclosed to the Law Commission by the Revenge Porn Helpline.

61 Figures disclosed to the Law Commission by the Revenge Porn Helpline; note that these are not included in the total calls noted above.

62 This term was introduced to the public in December 2013, when an action was brought against the founder of UGotPosted, a website that posted such revenge pornography, using it to extort those depicted by charging them money for their removal. See S Pegg, "A matter of privacy or abuse? Revenge porn in the law" [2018] 7 *Criminal Law Review* 512.

63 Figures disclosed to the Law Commission by the Revenge Porn Helpline.

64 J Ledward and J Agate, "'Revenge Porn' and s 33: the story so far" (2017) *Entertainment Law Review* 40. If the images are shared, following blackmail, both offences could be charged.

65 Maria Miller MP has argued in favour of this: L Buchan, *Over 80 Labour MPs urge Theresa May to offer anonymity to revenge porn victims* (7 July 2018), available at https://www.independent.co.uk/news/uk/politics/revenge-porn-victims-anonymity-labour-urge-theresa-may-law-change-maria-miller-richard-burgon-dawn-a8434451.html; and L Buchan, *Revenge porn video of Love Island star and upskirting controversy put fresh pressure on government to tighten law* (22 June 2018), available at https://www.independent.co.uk/news/uk/politics/love-island-zara-mcdermott-video-upskirting-revenge-porn-laura-anderson-laws-latest-a8411406.html.

66 C McGlynn and E Rackley, "Image-Based Sexual Abuse" (2017) 37(3) *Oxford Journal of Legal Studies* 534, p 534.

67 In a recent study of the equivalent Scottish offence, 34% of disclosures occurred via Facebook and Facebook Messenger. See M Ellison, *Less than half revenge porn cases passed to prosecutors* (6 March 2018), available at https://www.bbc.co.uk/news/uk-scotland-42689607. It is also one of the most reported mediums for disclosures in England and Wales: see P Sherlock, *Revenge pornography victims as young as 11, investigation finds* (27 April 2016), available at https://www.bbc.co.uk/news/uk-england-36054273.

Meaning of "private" and "sexual"

10.55 Although a clear criminalisation rationale for section 33 was never fully articulated,[68] the constituent elements of the offence clearly centre on the sexual privacy intrusion to the victim caused by the disclosure. However, the fact that one of the constituent elements of the offence is the intent to cause distress suggests that the offence is designed to protect more than just sexual privacy, but also from intentions to cause harm or abuse.

Private

10.56 The offence applies whether or not the imagery was taken in public or in private, or whether the victim captured the imagery themselves, or it was taken by another.[69]

10.57 Section 35(2) of the CJCA 2015 defines a photograph or film as "private" where it "shows something that is not of a kind ordinarily seen in public".

10.58 The courts have interpreted "ordinarily seen in public" as referring to what is seen ordinarily in the physical world, rather than online or on television. This appears to be the approach assumed in the Explanatory Notes to the Act:

> the effect of subsection (2) is to exclude from the ambit of the offence a photograph or film that shows something that is of a kind ordinarily seen in public. This means that a photograph or film of something sexual (such as people kissing) would not fall within the ambit of the offence if what was shown was the kind of thing that might ordinarily take place in public.

10.59 Section 35(2) echoes the language in the offence of voyeurism found in sections 67 and 68 of the Sexual Offences Act 2003, where a "private act" is defined to include "a sexual act that is not of a kind ordinarily done in public".[70] This is discussed further in the section below.

10.60 However, acts or images that may be ordinarily seen in public may still be distressing when disclosed. For example, imagery of women and men wearing underwear or bikinis is the kind of "thing" that is ordinarily seen in public; many billboards and magazines carry such images every day. This does "take place" in public; people wear such clothing and kiss on beaches and in parks across the United Kingdom every summer. Nevertheless, it could be intensely distressing for some to have such videos or

---

68 See S Pegg, "A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512, p 516.

69 The Liberal Democrat party tabled an amendment to the Act in July 2014 which included a defence where there could be no reasonable expectation of privacy, but this was not adopted in the final Act. Such a defence could have applied in cases where sexually explicit "selfies" are shared. See A Phippen and J Agate, "New social media offences under the Criminal Justice and Courts Act and Serious Crime Act: the cultural context" (2015) *Entertainment Law Review* 82. A similar debate occurred in California concerning an equivalent offence, see H Schwarz, *California's revenge porn law, which notoriously didn't include selfies, now will* (27 August 2014), available at https://www.washingtonpost.com/blogs/govbeat/wp/2014/08/27/californias-revenge-porn-law-which-notoriously-didnt-include-selfies-now-will/?utm_term=.86d433940226.

70 Sexual Offences Act 2003, s 68(1)(c). The other contexts outlined are where "the person's genitals, buttocks or breasts are exposed or covered only with underwear" and where "the person is using a lavatory".

photographs disclosed, and it is inconsistent with other areas of law to say that such a photograph or film is not "private".

10.61 If it was intended to exclude this type of less explicit imagery from the scope of the offence, the better approach may have been to include more precise definitions and specify the types of intimate situations which the offence seeks to cover.[71]

Sexual

10.62 A photograph or film is defined as "sexual" where:

(1) it shows all or part of a person's exposed genitals or pubic area;

(2) it shows something a "reasonable person" would consider to be sexual because of its nature; or

(3) its content, taken as a whole, is such that a reasonable person would consider it to be sexual.[72]

10.63 The first example defined in the CJCA 2015 could be quite narrow when construed in isolation. For example, female breasts do not form part of female genitalia, and requiring that genitals or the pubic area be "exposed" could also fail to capture many forms of sexual imagery. However, the definitions in (2) and (3) are clearly wider in scope.

10.64 "Sexual" is also defined broadly in a different context: section 78 of the Sexual Offences Act 2003 ("SOA 2003"). In this provision, "penetration, touching or any other activity" is sexual "if a reasonable person would consider that: (a) whatever its circumstances or any person's purpose in relation to it, it is because of its nature sexual; or (b) because of its nature it may be sexual and because of its circumstances or the purposes of any person in relation to it (or both) it is sexual".

10.65 It is difficult to define precisely the types of imagery that would be found to be "sexual" under section 33 of the CJCA 2015.[73] Videos or images of a person having sex or performing oral sex would obviously come within the definition – they often involve showing a person's exposed genitals, and would be something a reasonable person would consider to be sexual. There have also been prosecutions for disclosing images of a woman's breasts to another,[74] though Gillespie questions if even this would constitute an offence if the picture was of a person sunbathing topless on a beach. A jury may not find the image to be sexual, and it could be argued not to be "private" as it is, according to Gillespie, the "kind" of thing that is ordinarily seen in public.[75]

---

71 See, eg the definition of "intimate situation" in the Abusive Behaviour and Sexual Harm (Scotland) Act 2016, s 3.

72 Criminal Justice and Courts Act 2015, s 35(3).

73 The term is defined in some Acts; for example, Sexual Offences Act, s 78.

74 *Marquis* (9 June 2015) Teesside magistrates' court (unreported), cited by S Pegg, "A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512, p 519.

75 A Gillespie, "'Trust me, it's only for me': 'revenge porn' and the criminal law" [2015] 11 *Criminal Law Review* 866, pp 869 to 870.

10.66 It is to be expected that such difficulties are going to continue to arise without a clearer definition of the meaning of "sexual" and "private", given the vagueness of the terms. It is currently unclear if the offence covers the taking and disclosure of a picture of a woman sunbathing topless in a park. It may or may not cover the disclosure of an intimate situation with a sexual partner lying on a bed in their underwear.

10.67 This is problematic, and arguably the law needs to be clearer about what intrusions of sexual privacy are within the scope of the offence. The infringement of privacy when a picture is taken publicly of a person striking a sexual pose in their swimwear on the beach, is a qualitatively different privacy intrusion to a picture of a person performing a sex act or naked in the privacy of their own room, but the terms "sexual" and "private" are so vague that without further definition or qualification, it is difficult to know what type of private, sexual photograph will fall within the offence.

10.68 However, this must be balanced with the need for the provision to be flexible enough to enable the law to reflect changes in sexual practices and to reflect the harms caused to the victims,[76] similar to the broad approach to "sexual" in the SOA 2003. A possible alternative, McGlynn has suggested, is to exclude images where the victim has consented to the disclosure. This avoids a potentially exclusionary approach of specifying sexual privacy boundaries but also avoids the kind of confusion explained above. This argument was made by McGlynn and Rackley to the Scottish Parliament and is based on a similar approach in Illinois legislation.[77]

Excluded photographs and films

10.69 A photograph or film is defined in the CJCA 2015 as a "still or moving image in any form" that:

(1) appears to consist of or include one or more photographed or filmed images; and

(2) in fact consists of or includes one or more photographed or filmed images.[78]

10.70 Altered images are expressly included in this definition,[79] however, such images are excluded from the definition of a private sexual film or photograph where they:

(1) do not consist of or include a photograph or film that is itself private and sexual;

(2) are only private or sexual by virtue of the alteration or combination;

---

76 C McGlynn and E Rackley, "Image-Based Sexual Abuse" (2017) 37(3) *Oxford Journal of Legal Studies* 541.

77 C McGlynn and E Rackley, "Image-Based Sexual Abuse" (2017) 37(3) *Oxford Journal of Legal Studies* 541, p 542. See: C McGlynn and E Rackley, *Written submission to the Justice Committee – Abusive Behaviour and Sexual Harm (Scotland) Bill* (5 November 2015), available at http://www.parliament.scot/S4_JusticeCommittee/Inquiries/ABSH3._McGlynn_and_Rackley.pdf.

78 Criminal Justice and Courts Act 2015, s 34(4). Photographed and filmed images are in turn defined in ss 34(6) to (8).

79 Criminal Justice and Courts Act 2015, s 34(5).

(3) it is only by virtue of the alteration of combination that the relevant person is shown as part of, or with, whatever makes the photograph or film private and sexual.[80]

10.71 This means that if an image of a person is not private and sexual as originally created, and only becomes so due to a manipulation of the image, then disclosure of such an image will not constitute the section 33 offence. For example, if a person superimposed a photograph of another's face onto a pornographic image, this would fall outside the ambit of the offence.

10.72 Limiting the offence in this way has attracted criticism. As Gillespie argues, technology is now so advanced that altered or combined photographs can look realistic, and it can be difficult for viewers to spot fake images.[81] "Deepfake pornography"[82] is also now a growing phenomenon, and involves software which allows for the transposition of a person's face into pornographic videos.[83] The development of dedicated apps such as FakeApp have increased the ease of construction and dissemination of this type of imagery. Such imagery will only become more life-like and credible as the technology develops.[84]

10.73 Lord Marks raised concerns about such practices during debates in Parliament in 2016, where he sought to have the limitations in the legislation removed, noting:

> if a photograph or film as finished and published has the effect of a private and sexual image and is disclosed without the consent of the subject and with the relevant intent … that is ample reason to bring it within the section….[85] Distress may be caused to the victim where people that view the images think they are real and are unaware of the doctoring of the image.[86]

10.74 This view was not, however, shared by the government and the amendment was withdrawn. The Minister of State for the Home Office argued that:

---

80 Criminal Justice and Courts Act 2015, ss 35 (4) and (5).

81 A Gillespie, "'Trust me, it's only for me': 'revenge porn' and the criminal law" [2015] 11 *Criminal Law Review* 866, p 871.

82 D Sabbagh and S Ankel, *Call for upskirting bill to include "deepfake" pornography ban* (21 June 2018), available at https://www.theguardian.com/world/2018/jun/21/call-for-upskirting-bill-to-include-deepfake-pornography-ban.)

83 P Grannum, *New Sexually Explicit App Allows you to Paste Anyone's Face onto the Star's Body* (27 January 2018), available at https://www.inquisitr.com/4757404/new-porn-app-allows-you-to-paste-anyones-face-onto-the-stars-body/.

84 The creator of this particular application has said that he wants to "improve it to the point where prospective users can simply select a video on their computer, download a neural network correlated to a certain face from a publicly available library, and swap the video with a different face with the press of one button". See P Grannum, *New Sexually Explicit App Allows You to Paste Anyone's Face onto the Star's Body* (27 January 2018), available at https://www.inquisitr.com/4757404/new-porn-app-allows-you-to-paste-anyones-face-onto-the-stars-body/.

85 *Hansard* (HL), 16 November 2016, vol 776, col 1437 (Lord Marks of Henley-on-Thames).

86 *Hansard* (HL), 16 November 2016, vol 776, col 1445 (Lord Marks of Henley-on-Thames).

the disclosure of such an image, though still distressing, does not have the potential to cause the same degree of harm as the disclosure of an undoctored photograph showing images of the kind referred to in section 35(3) of the 2015 Act.[87]

10.75 There is a distinction to be drawn between a fake private and sexual image, and a real one which captures something that a person has actually done. While both engage the person's right to privacy and right to data protection, disclosing actual footage is distinguishable from the perspective of privacy.[88] If the disclosure is of conduct which the victim has personally engaged in, to use Lord Hoffman's approach that opened this Chapter, it is revealing an aspect of a person's "private life" without their consent: the act itself is part of their private life. However, if the image is fake, the act portrayed is not an actual part of their "private life" and may be more of a misrepresentation rather than an invasion of privacy. The humiliation and distress felt by the victim, however, may well be the same.

10.76 Social media platforms, such as Twitter, have made public announcements about removing such content from their sites and/or it being against their guidelines.[89] This indicates that internet service providers are taking this activity increasingly seriously, and the law needs to keep pace. Other jurisdictions, such as some states of Australia, do not exclude the non-consensual disclosure of altered imagery.[90]

10.77 While at present, such altered imagery falls outside the scope of section 33, other charges could be pursued in these circumstances. The offence in section 170 of the DPA 2018 (knowingly or recklessly disclosing personal data without consent) may be applicable,[91] as could the false communication offences in section 127(2) of the CA 2003 and section 1 of the Malicious Communications Act 1988 ("MCA 1988"), as discussed in Chapter 11. In the latter case, the maximum penalty would be equivalent to the offence in section 33 of the CJCA 2015 (two years' imprisonment). However, as discussed in Chapter 4, this offence may not be available where an electronic communication is not sent directly to a person.

10.78 These alternative offences may not be sufficient, as they fail to convey the seriousness of such offending and the harm that non-consensual disclosure of altered images –

---

87 *Hansard* (HL), 16 November 2016, vol 776, col 1443 (The Minister of State, Home Office (Baroness Williams of Trafford)), cited by S Pegg "'A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512, p 521.

88 Although the altered image could include private information (eg a private photograph of the victim) or personal data (in that the person is identifiable). See Articles 7 and 8 of the EU Charter of Fundamental Rights.

89 See, eg A Mak, "Twitter is Rolling Out Stricter Rules on Sexual Abuse, Violence, and Hate Speech" (18 October 2017), available at http://www.slate.com/blogs/future_tense/2017/10/18/twitter_s_new_rules_regulate_sexual_abuse_hate_and_violence.html?via=gdpr-consent.

90 For example, in the Australian Capital Territory, section 72A of the *Crimes Act 1900* defines an intimate image for the purposes of the offence, which "includes an image, in any form, that has been altered to appear to show any of the things mentioned in paragraph (a)". In New South Wales, section 91N of the *Crimes Act 1900* includes "an image, whether or not altered".

91 This would apply, for example, if a defendant tricked the user into giving him access to his social media profile, from which he took the photograph (personal data) for the fake pornographic image.

which can identity the person it depicts – can cause to its victims. They also fail to affix the appropriate label to such conduct.

Meaning of "disclose"

10.79 A photograph or film is "disclosed" to a person if the defendant "by any means… gives or shows it to the person or makes it available to the person."[92]

10.80 The concept of "make available" can be widely interpreted to apply to both online and offline forms of communication. The CPS guidelines note that this would include sharing by text or email, uploading images to the web, or physically showing someone the photograph or film.[93] This is consistent with the interpretation of "making available" in other contexts.[94] Gillespie argues that the words "makes available" are broad enough to embrace many forms of technological disclosures, and should equally be interpreted broadly in the context of section 33.[95]

10.81 The CPS guidelines further state that "the offence applies equally online and offline and to images which are shared by electronic means or in a more traditional way".[96]

10.82 In the modern era, online disclosure appears to be a more frequent occurrence, though there are cases of offline distribution. For example, Luke Brimson from Bristol printed out sexual images of a woman and handed them out in a supermarket.[97]

10.83 It is not clear on the face of the provision if the offence is only committed where the disclosure has resulted in a viewing by another person. Pegg argues that this need not occur, and that the offence can be committed even where the image is not viewed or seen by a recipient.[98] This would be a similar approach to the sending of an indecent, obscene or false communication under section 127(1) and (2) of the CA 2003. If this analogy is accepted, it therefore may be possible for an offence to have occurred if a private sexual image is posted online but deleted before anyone has actually seen the

---

92 Criminal Justice and Courts Act 2015, s 34(2).

93 Crown Prosecution Service, *Guidelines on prosecuting the offence of disclosing private sexual photographs and films* (24 January 2017), available at https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines-prosecuting-offence-disclosing-private-sexual.

94 See, eg *R v Dooley* [2005] EWCA Crim 3093; [2006] 1 WLR 775 in the context of child sexual abuse imagery, where the term "make available" was applied in relation to "peer-to-peer networks" by way of saving images in a "my shared folder".

95 A Gillespie, "'Trust me, it's only for me': 'revenge porn' and the criminal law" [2015] 11 *Criminal Law Review* 866, p 868. See also *R v Fellows* [1997] 2 All ER 548, where the first appellant operated a computer archive containing indecent photographs of children, and he provided the password to certain individuals who could either download or upload from the folder. Such actions would no doubt constitute a disclosure in the context of section 33 of the CJCA 2015, where private sexual images are made available by the provision of the password.

96 Crown Prosecution Service, *Guidelines on prosecuting the offence of disclosing private sexual photographs and films* (24 January 2017), available at https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines-prosecuting-offence-disclosing-private-sexual.

97 Discussed in S Pegg, "A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512, p 517; and see BBC, *Shirehampton man charged with "revenge porn" offence* (22 July 2015), available at https://www.bbc.co.uk/news/uk-england-bristol-33622584.

98 S Pegg, "A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512, p 517.

image. The image is still being "made available" to a person or persons, even if those people do not actually see it. Given the distress caused to the victim by way of disclosure of the image may still be significant, despite no one actually seeing the image, it is likely that this may still be an offence. Of course, in practice, a viewing will usually have occurred, which is why it comes to the attention of the authorities.

10.84 Even in cases of temporary disclosure, such as a Snapchat message, a disclosure would still occur, as the image would be made available to another, even if the image was automatically deleted after opening or even if it was not opened at all. Note however, that even with apps such as Snapchat, receivers may take a screenshot of an image that creates a permanent record.

10.85 Those that re-tweet or forward such photographs or films would also disclose for the purposes of the CJCA 2015. Section 34(3) states that something that is given, shown or made available to a person is disclosed "whether or not it has previously been given, shown or made available to the person". Whether they are prosecuted, however, will depend on whether they intend to cause distress.

Disclosures to the person depicted in the private and sexual image

10.86 One significant exclusion relates to disclosures of private and sexual photographs or films to the individual who appears in it. Section 33(2) of the CJCA 2015 states that such a disclosure is not an offence.

10.87 Gillespie speculates that the intention behind this provision may have been to avoid the criminalisation of consensual sharing of photographs or films between partners as part of their relationship.[99] He argues that any such steps taken to avoid criminalising this behaviour were unnecessary, however, as it would already not be an offence if it was done with the consent of the person in the image, and/or without an intention to cause distress.[100]

10.88 The result is that private and sexual photographs or films may be sent between sexual partners with intent to cause distress, without constituting an offence under section 33. This could occur, for example, where a couple (X and Y) are living apart, and X sends Y a sexually explicit photograph of herself, with instructions to delete it later. They later separate, and Y, some time later, sends the photo to X saying, "you'll always be mine when I've got this". As Gillespie succinctly notes, the fact that such a situation is excluded from the scope of the offence "is odd".[101] However, it is likely that a distinction was made based on the level of privacy invasion; in this example, Y has not breached X's privacy as he sent the image only to her and no-one else. This is distinct from, for example, if Y then sent that photograph to all of his friends, which would be a breach of X's privacy and therefore caught under the provision. The fact that parliament intended this to be a privacy offence (which, as noted in paragraph 10.53, has been the cause of

---

99 A Gillespie, "'Trust me, it's only for me': 'revenge porn' and the criminal law" [2015] 11 *Criminal Law Review* 866, p 867.

100 A Gillespie, "'Trust me, it's only for me': 'revenge porn' and the criminal law" [2015] 11 *Criminal Law Review* 866, p 867.

101 A Gillespie, "'Trust me, it's only for me': 'revenge porn' and the criminal law" [2015] 11 *Criminal Law Review* 866, p 867.

some debate), probably explains why it decided on the exclusion contained in section 33(2) of the CJCA 2015.

10.89 Other charges may be available, such as harassment (if there is a course of conduct) or communications offences such as section 1 of the MCA 1988 or section 127 of the CA 2003. If Y had covertly recorded sexual imagery of X, and then sent her the video, the offence of voyeurism could have been committed for the initial recording.[102] However, this begs an additional question as to whether such alternative charges are appropriate: section 127 of the CA 2003, for example, carries a less severe penalty which may not necessarily reflect the harm caused, and it may not be suitable to label the act as a communication offence, when it in fact carries different connotations (as a breach of privacy, for example).

Threat to disclose

10.90 Threats to disclose private and sexual images do not fall under the offence in section 33 of the CJCA 2015. A disclosure must actually be made for the offence to apply, as the offence focuses on invasions of privacy.

10.91 This can be contrasted with similar offences in other jurisdictions. In Scotland, section 2 of the Abusive Behaviour and Sexual Harm (Scotland) Act 2016 – the offence of disclosing, or threatening to disclose, an intimate photograph or film – can be committed by threats as well as actual disclosures of such imagery.

10.92 In England and Wales, threats to disclose private and sexual imagery could – depending on the circumstances – be prosecuted under section 127 of the CA 2003, section 1 MCA 1988, as blackmail (if there is a financial component), or harassment amongst other offences.

10.93 However, the lack of a specific offence covering threats to disclose non-consensual private and sexual imagery is concerning in an online context, given that it is very easy to follow through with the threat of sharing online.

10.94 Threats to disclose are most commonly experienced in the context of abusive relationships, such as in the example noted above.[103] Research currently being conducted by McGlynn suggests that while threats to disclose are reported to the police, charges are largely not laid, which indicates the law is inadequate in reflecting the harm caused to those receiving threats that can realistically, and easily, be carried out.

---

102 See Sexual Offences Act 2003, s 67(3).

103 Evidence from Australia highlights threats are common (and just slightly less than distribution victimisation): 10.6% experienced distribution of images without consent; 8.6% threats (see Powell and others, "Image-Based Sexual Abuse", in W DeKeseredy and M Dragiewicz, *Routledge Handbook of Critical Criminology* (2nd ed, 2018) pp 305 to 315. See also a report which stated that 9.6% of Australian adults surveyed reported that someone had threatened to share nude or semi-nude images online: A Powell and N Henry, *Digital Harassment and Abuse of Adult Australians: A Summary Report* (2015), available at https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=2ahUKEwiI1JafiJXdAhUMDcAKHUZcBTcQFjAJegQIAxAC&url=https%3A%2F%2Fresearch.techandme.com.au%2Fwp-content%2Fuploads%2FREPORT_AustraliansExperiencesofDigitalHarassmentandAbuse.pdf&usg=AOvVaw2zlSrMvKPO-vLvxhBMYfKP.

The meaning of consent

10.95 The offence contrary to section 33 of the CJCA 2015 is only committed if the disclosure of the private and sexual image is without the consent of an individual who appears in the photograph or film. "Consent", according to section 33(7)(a) of the CJCA 2015, means both "general consent covering the disclosure, as well as consent to the particular disclosure".

10.96 The lack of a clear definition of consent in the CJCA 2015 has been criticised by academic commentators.[104]

10.97 Where there has been some form of ambiguous "general" consent to disclosure, difficulties may arise in determining the limits of this consent. For example, if a person shares a sexually explicit image of himself with a new sexual partner, within a particular social media group containing his ex-partner, in further sharing the image, the ex-partner could seek to argue that consent was provided for further distribution.[105] This would seem to stretch the notion of consent considerably, and it remains unclear how consent applies on the face of the law as it currently stands.

10.98 This could be contrasted with a situation where, for example, a person agrees to sharing private sexual imagery in a particular forum (amongst, say, a small group of "swingers" who regularly share sexual imagery of one another on a WhatsApp group), but where he or she expressly states that it should not be shared more widely. In this situation, the relevant person's consent to disclosure is specifically limited, and any further distribution would clearly constitute the offence, if the sharer can be shown to have had the necessary intention to cause distress. There is no reason why a qualified/conditional consent such as this would not be protected within the terms of the offence.[106]

10.99 It has also been argued that the lack of a specific definition of consent in section 33 may cause difficulties for courts in directing juries. For example, difficulties may arise where a person gives consent to a particular disclosure while intoxicated, or where the consent is given in the context of an emotionally abusive and controlling relationship, or given but later retracted.[107] It is likely that the courts would draw on the case law on "consent" in the context of the Sexual Offences Act 2003 to inform these directions.

---

104 See S Pegg, "A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512, pp 521 to 523.

105 See, eg the case of Tiziana Cantone, who sent videos of herself performing sex acts on a number of men to her ex-boyfriend and others on a WhatsApp group, which were then subsequently shared widely. See R Warren, *A Mother Wants the Internet to Forget Italy's Most Viral Sex Tape* (16 May 2018), available at https://www.theatlantic.com/technology/archive/2018/05/tiziana-cantone-suicide-right-to-be-forgotten/559289/.

106 Discussed by S Pegg, "A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512, p 522.

107 For example, S Pegg, "A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512, pp 521 to 523.

10.100 The fact that the Act is silent on *who* must give consent may create further difficulties in practice.[108] For example, in a recent case in Ireland, a 17-year-old girl performed fellatio on a man while intoxicated at a concert. Photos and videos of the acts were taken by many attendees and went viral on social media. Other members of the crowd were visible in these photos and videos. Even if the couple performing these acts in public agreed to the recording and distribution (which was not the case on the facts; the girl, at least, was hospitalised due to the distress caused) and provided "general consent" for disclosure, the section 33 offence, as well as others, could still have been committed.[109]

10.101 If other members of the crowd were visible, and perhaps staring at what was unfolding in front of them, it is not difficult to imagine how it could be distressing for these "spectators" to be seen and associated with the footage. If someone shared the footage with the intention of causing them distress, the offence in section 33 would be formally committed. The spectators appear in the images (even if not engaged in the sexual acts), and they do not provide consent to the sharing (for the purposes of section 33(1)(a)).

Intention to cause distress

10.102 Section 33 of the CJCA 2015 requires that the prosecution prove that the defendant disclosed the private sexual photograph or film with the intention to cause distress to an individual who appears in the photograph or film.

10.103 Disclosure alone of the private, sexual image is not sufficient to infer intent.[110] More is required than merely showing that distress "was a natural and probable consequence of the disclosure".[111]

10.104 This ensures that only those that intend their victim to be distressed will be caught by the offence, but it excludes those that act with indifference or for a different purpose entirely (such as financial gain or to humiliate the victim). An individual could have been forwarded a private sexual video of two strangers, and may share it more widely because he or she thinks a particular scene is funny, without even considering the likely impact on the individuals in the video or whether there was consent for initial disclosure.

---

108 A Gillespie, "'Trust me, it's only for me': 'revenge porn' and the criminal law" [2015] 11 *Criminal Law Review* 866, p 871.

109 If this occurred in the United Kingdom, recording a 17-year-old performing such an act would constitute the offence of making an indecent photograph of a child under section 1 of the Protection of Children Act 1978. Any further possession or distribution would also constitute offences for child sexual abuse images. If both parties were over the age of 18, the people recording such acts would not commit the offence of voyeurism, as it was not a "private act", (see Sexual Offences Act 2003, s 68) but would potentially commit the offence in section 33. Even if she had the capacity to give consent to the sexual act itself (which was an act of outraging public decency), she may not have given consent to the recording and subsequent disclosure. While the act occurred in public, it was not one that is "ordinarily seen in public", as discussed above, and thus any footage of it would constitute a private and sexual photograph or video. Liability would therefore turn on whether there was an intention to cause distress. Those that share the image could also potentially commit the offence in section 127(1) of the Communications Act 2003.

110 See Criminal Justice and Courts Act 2015, s 33(8).

111 Criminal Justice and Courts Act 2015, s 33(8).

This would not constitute an offence under section 33, though it may be another offence (such as under section 127 of the CA 2003).

10.105 This can be contrasted with the equivalent Scottish offence, where recklessness will suffice.[112]

10.106 While Pegg has argued that the high threshold of intention to cause distress is not proving difficult in practice,[113] prosecution statistics and research have suggested otherwise. As noted above, there is a significant level of attrition of section 33 cases from reporting to prosecution, with one of the reasons cited being "evidential" challenges, which include having to meet the distress threshold. Research conducted by Bond and Tyrell, who interviewed 783 police officers about section 33 offences, found a "significant lack of understanding and confidence felt by police" in investigating this type of conduct, with 97% of police revealing they had received no training on the issue.[114] As McGlynn noted, "this suggests that there is a lack of understanding of the law, and that provisions such as the intent to cause distress may be impeding investigations". McGlynn's recent research with police has also indicated that a lack of evidence to reach the intent to cause distress threshold is a reason for section 33 charges being dropped.

Defences

10.107 There are three defences provided to the section 33 offence in the CJCA 2015.

10.108 The first, in section 33(3), is if the person charged reasonably believed that disclosing the image or film was "necessary for the purposes of preventing, detecting or investigating crime". This defence is also available in section 170(2)(a) of the DPA 2018, and section 1B of the Protection of Children Act 1978, and could be relied upon by law enforcement as well as members of the public. The person relying on this particular defence would have to prove their reasonable belief in the necessity of the disclosure, and academic authority is already divided as to whether this is a legal or evidential burden.[115]

10.109 The second defence is a public interest defence contained in section 33(4) and relates to the disclosure made "in the course of, or with a view to, the publication of journalistic material". The person charged must have "reasonably believed" that the publication of the journalistic material was in the public interest.

10.110 "Publication" of journalistic material is defined in section 33(7)(b) as "disclosure to the public at large or to a section of the public".

---

112 Abusive Behaviour and Sexual Harm (Scotland) Act 2016, s 2(1)(b).

113 See S Pegg, "A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512, pp 524 to 525.

114 E Bond and K Tyrell, "Understanding Revenge Pornography: A National Survey of Police Officers and Staff in England and Wales" (2018) *Journal of Interpersonal Violence*.

115 See, eg A Gillespie, "'Trust me, it's only for me': 'revenge porn' and the criminal law" [2015] 11 *Criminal Law Review* 866, p 868, and S Pegg, "A matter of privacy or abuse? Revenge porn and the law" [2018] 7 *Criminal Law Review* 512, p 525.

10.111 It is likely to be a rare case in which the publication of a private sexual photo or video of a person will be reasonably believed to be in the public interest.

10.112 Section 33(5) also provides a defence if the person charged reasonably believed the photograph or film had been "previously disclosed for reward", either by the individual depicted in it or another person, and the person "had no reason to believe that the previous disclosure for reward was made without the consent of the individual" depicted in the photograph or film.

10.113 If, for example, a person reasonably believed that a video was commercial pornography, and had no reason to believe there was a lack of consent for the previous disclosure, then the defence could be relied upon.[116]

VOYUERISM OFFENDING

10.114 Voyeurism, known colloquially as "peeping", in general terms refers to the unwanted observation or recording of another in circumstances where they would expect to have privacy; for example, while getting undressed, using a bathroom, or while engaged in a sexual act of some kind in a private place.

10.115 The offence of voyeurism was created by section 67 of the Sexual Offences Act 2003 ("SOA 2003").

10.116 There are several variations of the offence outlined in the SOA 2003:

(1) for the purpose of obtaining sexual gratification, observing another person doing a private act while knowing that the other person does not consent to being observed for sexual gratification;[117]

(2) installing equipment, or constructing or adapting a structure or part of a structure, with the intention of enabling the commission of the above offence;[118]

(3) operating equipment with the intention of enabling another person to observe, for the purpose of obtaining sexual gratification, a third person doing a private act, while knowing that the third person does not consent to the operating of the equipment with that intention;[119] and

(4) recording another person doing a private act, with the intention that the recorder or a third person will, for the purpose of obtaining sexual gratification, look at an

---

116 Crown Prosecution Service, *Guidelines on prosecuting the offence of disclosing private sexual photographs and films* (24 January 2017), available at https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines-prosecuting-offence-disclosing-private-sexual.

117 Sexual Offences Act 2003, s 67(1).

118 Sexual Offences Act 2003, s 67(4).

119 Sexual Offences Act 2003, s 67(2).

image of the subject doing the act, while knowing that the subject does not consent to this.[120]

10.117 The maximum penalty applicable to each of these offences is two years' imprisonment.[121]

10.118 It is important to note that the fault element of this offence is that the observing or recording must be for the purposes of sexual gratification. For example, A films her friend, B, masturbating in her bedroom and distributes that film amongst their group of heterosexual female friends for the purposes of embarrassment or humiliation – not sexual gratification. In these circumstances, A would not be committing an offence under section 67 of the SOA 2003[122] (although she may be committing other offences, such as under section 33 of the CJCA 2015).

10.119 A "private act" is further defined as where a person is in a place which, in the circumstances, would reasonably be expected to provide privacy, and the person's genitals, buttocks or female breasts are exposed or covered only with underwear, the person is using a lavatory, or the person is doing a sexual act that is not of a kind ordinarily done in public.[123] If, for example, a webcam was set up to record women getting undressed at a changing room at a gymnasium, and the footage was broadcast live, this would be an offence under section 67(3). The online broadcast is not an essential element of the offence, but may form the entirety of the perpetrators' motivation for making the recording.

10.120 Advanced technology has increased opportunities for, and ease and accuracy of, acts of voyeurism.[124] The internet has also allowed for voyeurism to occur on a much wider scale. Whether or not it is an offence that can be committed entirely online would depend on the interpretation of "place" in relation to online communication, and the law may struggle to adapt in this respect, for example, in determining whether the observation and recording of such acts could constitute an act of voyeurism. However, it is clear that an act of voyeurism could be at least partially committed in an online context. It could, for example, be "live-streamed" – video or audio coverage could be transmitted live – or recorded and uploaded later onto a website or social media platform.

10.121 A particularly horrific example of voyeurism in an online context occurred in the case of Matthew Falder. Amongst a variety of other offending, Falder set up secret cameras

120 Sexual Offences Act 2003, s 67(3).

121 Sexual Offences Act 2003, s 67(5).

122 P Rook and R Ward, *Rook and Ward on Sexual Offences: Law and Practice* (5th ed, 2016) para 15.91.

123 Sexual Offences Act 2003, s 68(1).

124 W McCann and others, "Upskirting: A Statutory Analysis of Legislative Responses to Video Voyeurism 10 Years Down the Road" (2017) *Criminal Justice Review* 2.

in homes and public toilets to film people undressing, and used the footage to blackmail the victims and trade with others online.[125]

10.122 It is unclear whether the meaning of "place" refers solely to a physical place. "Place" is not specifically defined in the SOA 2003, but it does not need to be a building or other structure, as reflected by the substitution of the word "place" for "structure" in the Sexual Offences Bill.[126] Is it possible, therefore, that a "place" could include an online place, not just an offline one? While a victim may be physically in a private place (her bedroom, for example), if she is live streaming herself conducting private acts, with hundreds of people watching, she is occupying a very different "place" – with different dimensions of privacy – from merely a bedroom. Whether a place can reasonably be expected to provide privacy is, the Court of Appeal has noted, an objective test,[127] and one for the jury to decide.[128]

10.123 The final form of "private act" contained in section 68(1)(c) of the SOA 2003, is similar to that of section 33 of the CJCA 2015, although it refers to acts "not of a kind ordinarily *done* in public" as opposed to ordinarily *seen* in public. However, when the recording or observation is done using online communication, it poses the question as to whether the "private act", if not falling within the other subsections, must be an act ordinarily done in the *physical* public world, or in the online public world. The two may be distinct, and acts which are not ordinarily done offline in public may be more ordinarily done online.

Upskirting Bill

10.124 A particular gap in the law of voyeurism has been identified recently in the context of behaviour commonly referred to as "upskirting". In Scotland, where this behaviour does constitute a criminal offence, it has been, in short, defined as occurring when a perpetrator operates equipment beneath the victim's clothing, with the intention of viewing the victim's genitals or buttocks – whether exposed or covered with underwear – for the purpose of obtaining sexual gratification or humiliating, distressing or alarming the victim.[129]

10.125 The gap in the current criminal law arises because where the offending conduct of taking an intimate recording occurs in an ordinary public context, such as where a person is riding on public transport, the "private act" element of the voyeurism offence under section 67 of the SOA 2003 cannot be established. The fault element of sexual gratification may also not be satisfied, where such images are taken and disseminated to humiliate, or to be humorous, for example.

---

125 T Larner and R Veralls, *'Worst of the worst' paedophile placed secret cameras in Welsh house to film people undressing* (19 February 2018), available at https://www.walesonline.co.uk/news/wales-news/worst-worst-paedophile-placed-secret-14308752.

126 P Rook and R Ward, *Rook and Ward on Sexual Offences: Law and Practice* (5th ed, 2016) 15.115.

127 *R v B* [2012] EWCA Crim 770 at [59]; [2013] 1 WLR 499, 514.

128 *R v Bassett* [2008] EWCA Crim 1174, [2009] 1 WLR 1032.

129 See Sexual Offences (Scotland) Act 2009, s 9.

10.126 Moreover, as Gillespie notes, where a photograph is taken up a person's skirt in a public place such as a shopping centre, the person is not engaged in a "private act" because they are not exposing their genitals or buttocks (with underwear or otherwise) in that place; they are covered by clothing. Such images or recordings would fall outside the current voyeurism offence because they would not be considered to be a "private act". This differs from, for example, undressing in a changing room, the recording of which would fall within the voyeurism offence.[130]

10.127 This distinction was exemplified in the case of *R v Ching Choi*,[131] in which the charges related to the common law offence of outraging public decency. The Court of Appeal dismissed Choi's appeal against conviction, after he was found to have filmed a woman on the lavatory in a Chinese supermarket, from the partition of an adjoining cubicle.

10.128 The gap in the current legislation emerged in the case of *R v Henderson*,[132] where some of the charges related to photographs taken by the appellant on his mobile phone of a 14-year-old girl sitting on a step in a public place, and up a woman's skirt in a shop. Neither incident was a voyeurism offence under the SOA 2003; they did not involve a private act, nor were they in places which "would reasonably be expected to provide privacy".[133]

10.129 The common law offence of outraging public decency may also be applicable in some upskirting contexts, but the requirement that the act occur in a "public place" arguably also excludes certain contexts.[134] For example, in *R v Walker*,[135] a man exposing himself to a daughter and another girl in the sitting room of his house was found to not be "in public".

10.130 In response to the concern about a gap in the law, the Voyeurism (Offences) (No. 2) Bill[136] has been introduced into Parliament. The Bill would create new offences where a person operates equipment or records an image beneath the clothing of another person to observe or record the person's genitals or buttocks (whether exposed or covered with underwear), or the underwear covering the person's genitals or buttocks, in circumstances where the genitals, buttocks or underwear would not otherwise be visible.[137]

10.131 Other elements of the offence are that the conduct is undertaken without the person's consent, or a reasonable belief in that consent, and that the observing or recording is

---

130 A Gillespie, "'Upskirts' and 'down-blouses': voyeurism and the law" [2008] *Criminal Law Review* 370.

131 [1999] EWCA Crim 1279.

132 [2006] EWCA Crim 3264.

133 Although there would be alternative offences available. For discussion see D Selfe, "Voyeurism – early developments in a new offence" (2007) 174 *Criminal Lawyer* 4.

134 We discuss this offence in more detail in our 2015 report: Simplification of Criminal Law: Public Nuisance and Outraging Public Decency (2015) Law Com No 358.

135 [1996] 1 Cr App R 111.

136 Voyeurism (Offences) (No. 2) Bill (2017-2019), cl 1(2).

137 Voyeurism (Offences) (No. 2) Bill (2017-2019).

done for the sexual gratification of the defendant or another, or to humiliate, alarm or distress the victim.

10.132 The proposed maximum penalty in the Bill is two years' imprisonment.[138]

10.133 The Bill does not cover another form of voyeurism – that of "down-blousing", where a person takes photographs or records another from above, focusing on the other person's cleavage, bra and breasts.[139] This could also potentially be done through the use of online equipment, and is another example of the law playing catch up with the way advancements in technology increase the opportunities to commit different types of privacy related offences.

ONLINE CONSIDERATIONS

10.134 The online world is connecting people in ways that we could hardly have imagined only a few decades ago. It has brought email and instant messaging, and instantly accessible "googled" knowledge. We can hold simultaneous video calls with groups of loved ones in multiple locations across the globe, with free applications that can be downloaded on any laptop, tablet or phone. Further, online dating is now, according to some studies, the most popular way to meet partners.[140]

10.135 This hyperconnected world has also wrought far-reaching and significant challenges for, amongst other things, the right to privacy. Online platforms have encouraged a sharing economy that has resulted in the "privacy paradox", where users care about their privacy online, but do not apply these concerns to their corresponding usage behaviour.

10.136 Many today share their lives on social media, sometimes with hugely damaging consequences. For example, there are many reports of burglaries after social media users have publicly disclosed information about being away on holiday. Individuals of varying ages are also now quite willing to use technology to capture and store sexual imagery of themselves. A study by McAfee found that nearly 50% of adults admitted using their mobile devices to share or receive intimate content.[141] A Cosmopolitan magazine poll of 850 readers found that almost 90% of readers have taken nude photos of themselves at some point.[142] For many it is a positive experience, assisting in

---

138 Voyeurism (Offences) (No. 2) Bill (2017-2019), cl 1(2).

139 A Gillespie, "'Upskirts' and 'down-blouses': voyeurism and the law" [2008] *Criminal Law Review* 370.

140 The Knot, *Only 1 in 3 US Marriage Proposals are a Surprise; Engagement Ring Spend Rises, According to The Knot 2017 Jewelry and Engagement Study* (9 November 2017) available at, https://www.prnewswire.com/news-releases/only-1-in-3-us-marriage-proposals-are-a-surprise-engagement-ring-spend-rises-according-to-the-knot-2017-jewelry--engagement-study-300552669.html. See also MJ Rosenfeld and RJ Thomas, "Searching for a Mate: The Rise of the Internet as a Social Intermediary" (2012) 77(4) *American Sociological Review* 523, available at: https://web.stanford.edu/~mrosenfe/Rosenfeld_How_Couples_Meet_Working_Paper.pdf.

141 Cited in Scientific American, *Sext much? If so, you're not alone*, available at https://www.scientificamerican.com/article/sext-much-if-so-youre-not-alone/.

142 E Barker, *Cosmo Survey: 9 out of 10 Millennial Women Take Naked Photos* (3 September 2014), available at https://www.cosmopolitan.com/sex-love/advice/a30675/ninety-percent-millennial-women-take-nude-photos-cosmo-survey/.

maintaining relationships, and in sexual expression.[143] But the storage of such data on internet-enabled devices carries the danger of accidental disclosure or unauthorised access.

10.137 Either of these phenomena (increased sharing of private information, and capturing of sexual imagery) can engage the criminal law, but will particularly do so when they collide.

10.138 Provisions such as section 33 of the CJCA 2015 connote an attempt to address some of these emerging privacy harms, but there are, once again, considerable legal and enforcement challenges when the offending is perpetrated online. Three of these difficulties include:

(1) privacy and crime in a privacy paradox: the online world is blurring the boundaries between public and private space, which can raise challenging questions in the prosecution of privacy offences;

(2) establishing the elements online: proving elements such as a lack of consent and intention, in a situation where there may be a lack of context for certain online communications, can render it difficult to prosecute offences such as section 33. Messages can be sent or forwarded quickly, with little thought, or in error;[144] and

(3) jurisdictional challenges: for those that intend to share private intimate details of others online, there are many ways through which they can rout communications to complicate and frustrate investigative efforts.

---

143 E Hunt, *Nude selfies: what if they are just an ordinary part of teenage life?* (31 August 2016), available at https://www.theguardian.com/australia-news/2016/sep/01/nude-selfies-what-if-they-are-just-an-ordinary-part-of-teenage-life.

144 There are a number of incidents where even politicians and public figures have mistakenly sent such messages. See, eg B Kentish, *Theresa May's Chief of Staff Gavin Barwell says he 'regrets' replying to porn tweet* (14 February 2018), available at https://www.independent.co.uk/news/uk/politics/theresa-may-gavin-barwell-porn-twitter-downing-street-chief-staff-reply-twinky69-a8210476.html.

Privacy and crime in a "privacy paradox"

Example 1

Maxine is a journalism student who has recently heard of a platform called "Randomchatting", an online chat website. After the user gives access to their webcam and microphone, the platform randomly pairs users with another individual, who could be anywhere in the world. Users can – with the click of a button – swap to another user if they wish to engage in another conversation.

Maxine has heard that most men abuse the platform by engaging in public exhibitionism and masturbating on screen. She thinks it would make an interesting topic for her coursework to write an article with empirical data that she gathers from use of the website.

She logs on, and captures a screen shot of every person that she is paired with. After one hour on the platform, and over one hundred "Randomchatting" conversations, she finds that almost 40% of the users were men masturbating. She is shocked, particularly as she also encountered many children on the platform who must have also seen these graphic live videos.

She decides that her findings are important enough for a post on her personal blog, and hopes it may get picked up by national media. She eloquently and graphically documents her time on Randomchatting and attaches all the "screen grabs" she took, including of the men who were performing sexual acts on the website. Many users are readily identifiable from the published photographs, and she states in the blog that those who were masturbating on screen should be "named and shamed".

Her blog post does get some media coverage. It comes to the attention of one of the users, Tom, that he was pictured while connected to Maxine via Randomchatting. He is horrified. Tom had actually been masturbating with another "chat" partner, in a consensually agreed and mutual arrangement, before he accidentally pressed the button for the next user. He was mortified at the time that Maxine had seen him, and even more so that the screengrab has been publicly disclosed in this way. He complains to police and wants her to remove his image from her blog.

Analysis

10.139 There are many websites like "Randomchatting" which facilitate random online video chat, and many individuals do use them to engage in sexual exhibitionism as described in the example above.[145]

[145] See M Farokhmanesh, *What remains of Chatroulette: It's gone to the do(n)gs* (14 February 2018), available at https://www.theverge.com/2018/2/14/16381942/chatroulette-webcam-chat-male-community. For academic studies of these platforms, see T Gregory, "Colonising antinormative sex: the flexibility of post-porn heterosex in random webcam sex" (2018) 21(4) *Sexualities* 657 and D Kreps, "Foucault, Exhibitionism

10.140 These platforms are a good illustration of how the distinction between public and private spaces can quickly collapse in the online environment. Few would argue there is any public interest in prosecuting two consenting adults who meet online and agree to perform "private" sex acts in front of each other via their webcams.[146] However, they are doing so over a public communications network, using a website accessible to children and others, where one mistaken touch of a button could involve that person technically committing a string of criminal offences, and in more than one jurisdiction.[147]

10.141 This example also illustrates the ease with which individuals can commit criminal offences by publishing private information about others – even where they think the latter are committing criminal offences. This is now a significant risk with the rise in "paedophile hunter groups" on social media,[148] where disclosure of information about a person, in conjunction with false allegations, could constitute civil as well as criminal offences.

10.142 Maxine may have had good intentions but may also have committed criminal offences.

10.143 By disclosing the personal data of all the individuals from her screengrabs, her actions may come within the offence in section 170 of the DPA 2018,[149] though this would depend on who the data controller was in the scenario,[150] and she may also be able to rely on a defence.[151]

10.144 A stronger argument could be made that she committed the offence in section 33 of the CJCA 2015. She disclosed a private sexual photograph of several men, and appeared to intend to cause them distress. She could try to rely on the journalism

---

and Voyeurism on Chatroulette" cited in F Sudweeks, H Hrachovec and C Ess (eds), *Proceedings: Cultural Attitudes Towards Communication and Technology* (2010) pp 207 to 216.

146 This could actually constitute an offence under section 127 of the Communications Act 2003 (knowingly sending by means of a public electronic communications network a message that is indecent or obscene).

147 In reality, sex acts over websites usually only come to the attention of police in cases of "sextortion" and blackmail. See The Local, *Norwegian police agency investigates online extortion after man's suicide* (5 March 2018), available at https://www.thelocal.no/20180305/norwegian-police-agency-investigates-online-extortion-after-mans-suicide; M Bagot, *Online blackmail scam: Thousands of British teenagers targeted by con artists* (17 August 2013), available at https://www.mirror.co.uk/news/uk-news/online-blackmail-scam-thousands-british-2176956; and N Sommerlad, *"Sextortion" gangs blackmail 30 teenagers a day by luring them into webcam sex acts using fake women's profiles* (5 March 2017), available at https://www.mirror.co.uk/news/uk-news/cyber-sex-gangs-blackmail-30-9972341.

148 Press Association, *Evidence from "paedophile hunters" used to charge suspects 150 times in last year* (10 April 2018), available at https://www.theguardian.com/uk-news/2018/apr/10/paedophile-hunters-vigilantes-police-evidence-grooming.

149 Knowingly or recklessly disclosing personal data without the consent of the data controller. She could not rely on a household exemption due to the public nature of the web publication. See Case C-101/01 *Bodil Lindqvist* [2003] ECR I-596.

150 The website owner would be data controller of eg communications data associated with the video chats and such information constituting personal data. On IP addresses as personal data, see Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECR I-779. It is likely that the users themselves would be found to be data controllers with respect to any screengrabs taken of individuals using the service.

151 For example, she could claim that she acted in "a reasonable belief" that she had "a legal right to do the obtaining, disclosing, procuring or retaining": Data Protection Act 2018, s 170(3)(a)). She could also claim that she was acting "for the purposes of preventing or detecting crime" (Data Protection Act 2018, s 170(2)(a)) though this is not clear on the facts above.

defence,[152] or possibly make an argument that she was acting to prevent or detect crime, though that motive was not clear on the facts stated above.[153]

10.145 Of course, many of the men on the platform may have been themselves committing criminal offences – either sexual offences or communications offences[154] – whether they were physically in the jurisdiction when they were broadcasting their sexual acts, or possibly even if their communications were visible and received by people such as Maxine in England and Wales.[155]

Establishing the elements online

10.146 Central to the offence in section 33 of the CJCA 2015 are the concepts of "private", "sexual", "consent" and an intention to cause distress. Privacy and consent, in particular, are challenging concepts to define and apply in any context, but all elements can be particularly difficult to apply where the offending is perpetrated over the internet, where messages can be sent or forwarded with little contextual knowledge of content.

Example 2

Joe and Janet like to record themselves dressing up and role playing in their sexual activities.

Joe has recently been learning how to create webpages for his business, and decides it would be useful to have them saved in one place and accessible from anywhere, in case he and Janet ever lose or break their phones. He decides to create a password protected webpage for the videos and uploads a number of them into cloud-based storage.

Unfortunately, Joe makes an error in uploading and the videos are made publicly accessible on the website. They quickly begin trending, and an internet meme is created with a private and sexual picture of Joe and Janet.

Hundreds of people share hyperlinks to the webpage on social media, and others download the videos, and upload them to pornographic websites where they are viewed thousands of times.

---

152 Criminal Justice and Courts Act 2015, s 33(4).

153 Criminal Justice and Courts Act 2015, s 33(3).

154 eg engaging in sexual activity in the presence of a child (Sexual Offences Act 2003, s 11); causing a child to watch a sexual act (Sexual Offences Act 2003, s 12); sexual communication with a child (Sexual Offences Act 2003, s 15A); exposure with intent to cause distress (Sexual Offences Act 2003, s 66); obscene publications (Obscene Publications Act 1959, s 2); Communications Act 2003, s 127; and Malicious Communications Act 1988, s 1.

155 In either situation it could be argued that a "substantial measure" of the criminality occurred in England and Wales.

Analysis

10.147 It is not clear that any offence under section 33 of the CJCA 2015 has been committed in this situation.

10.148 Despite the widespread availability of the videos, the recordings would still constitute "private" images for the purposes of the Act.[156] Individuals having sex is not the "kind" of "thing" that is "ordinarily seen in public".

10.149 What would be less clear to those sharing the videos is whether there was general consent from Joe and Janet for such sharing. In reality, there was no general consent to the sharing, even if it appeared that they were deliberately made available on their webpage.

10.150 Nevertheless, any potential prosecution may fail here if it cannot be proven that the sharers intended to cause distress. As the CPS guidelines note:

> anyone who re-tweets or forwards without consent, a private sexual photograph or film would only be committing an offence if the purpose, or one of the purposes, was to cause distress to the individual depicted in the photograph or film who had not consented to the disclosure. For example, anyone who sends the message only because he or she thought it was funny would not be committing the offence.[157]

10.151 In addition, those individuals who posted website URI[158] links to the videos would not commit a copyright offence, unless it could reasonably have been known that the linked-to published works were unauthorised, and the linking was for gain.[159] It may even be difficult to make out a criminal copyright offence against those that download and share the videos on pornographic websites.[160]

10.152 Charges of publishing obscene content, or distributing messages of an obscene or indecent character (section 127 of the CA 2003) would be unlikely in this situation.

---

156 It may be more difficult to establish a reasonable expectation of privacy more generally in relation to the information for the purposes of eg the tort of misuse of private information, though the fact that this was done unwittingly would be an important consideration. See, eg *GYH v Persons Unknown* [2017] EWHC 3360 (Admin) at [33], where it was said that "someone who makes information about herself public may have no reasonable expectation of privacy in relation to that or similar information and hence no right to prevent others from disclosing it". If Joe and Janet were identifiable from the imagery, they would also be able to avail of data protection remedies, as any sharing of the videos would constitute a processing of personal data.

157 Crown Prosecution Service, *Guidelines on prosecuting the offence of disclosing private sexual photographs and films* (24 January 2017), available at https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines-prosecuting-offence-disclosing-private-sexual.

158 URI: Uniform Resource Identifier.

159 See, eg Case C-466/12 *Svensson and others* [2014] ECR I-76; and Case C-160/15 *GS Media v Sanoma Media Netherlands and Others* [2016] ECR I-644.

160 Section 107(2) of the Copyright Designs and Patents Act 1988 criminalises communication of a copyright protected work to the public, but only if the defendant knows or has reason to believe that he is infringing copyright in the work, and either intends to make a gain for himself or another, or knows or has reason to believe that communicating the work to the public will cause loss to the owner of the copyright, or will expose the owner of the copyright to a risk of a loss.

10.153 In this case, the most important thing for Janet and Joe is for the distribution of the images to stop. Joe could limit the distribution by removing the videos from his website, or by properly password protecting the content. This would prevent the access via hyperlinking. However, the videos would still be available on the pornographic websites.

10.154 While Joe and Janet could use data protection remedies (such as the right to erasure), and seek injunctions for harassment or misuse of private information, these avenues can be costly and time-consuming. Moreover, ultimately they may not be particularly effective at stopping the distribution, particularly where the images have already "gone viral" or the websites are based abroad and not responding to legal requests. Such remedies would also likely be limited to the United Kingdom and would be difficult to enforce cross-jurisdictionally.

10.155 Cases like that of Tiziana Cantone illustrate the devastating consequences for victims where private sexual images "go viral" and are shared as widely as this.[161]

Doxing

Example 3

Tanya is a film writer and outspoken advocate for gender equality with a high profile on Twitter. She spearheads a campaign for better representation of women in superhero films and her timeline is swamped with numerous threats, including explicit and detailed death threats.

She creates a Facebook group, which anyone can ask to join. She is the administrator of that group and personally accepts requests to join. The purpose of the Facebook group was to organise a protest on the street where her business resides. She posts her professional address in the group, so that members can attend the protest.

One member of the group, Ted, re-posts the post with her address onto his own Facebook wall, which is seen by his 2,000 Facebook friends, so they may attend the protest.

Tanya is very concerned about the re-posting of her professional address by Ted and is convinced that someone who had previously threatened her online might use that data to come and murder her at work.

[161] Cantone recorded sexually explicit videos of herself engaged in sexual activities with a number of men, and sent them to her ex-boyfriend and four other people in a WhatsApp group. They were then further disclosed by members in the group. The videos went viral and memes were developed from some of her comments in the videos; her phrases were printed on phone cases and T-shirts. Cantone was in the process of changing her name and went into hiding in Tuscany, but soon thereafter committed suicide. See R Warren, *A Mother Wants the Internet to Forget Italy's Most Viral Sex Tape* (16 May 2018), available at https://www.theatlantic.com/technology/archive/2018/05/tiziana-cantone-suicide-right-to-be-forgotten/559289/.

Analysis

10.156 As noted above, Tanya's professional address is a form of location data and could constitute "personal data" for the purposes of section 170 of the DPA 2018.

10.157 Tanya may not necessarily have consented to her professional address being made public to such a large group of people, and of such varying political views. By posting on the Facebook group which she controlled, such that members were personally accepted by her, she may not be consenting to a wider dissemination of that data.

10.158 However, Ted may argue that her posting on Facebook indicated consent to disclose that data.

10.159 Facebook would be the controller of this data for the purposes of the DPA 2018 and GDPR and may have obligations under the DPA 2018.[162]

Jurisdictional challenges

10.160 The internet has facilitated numerous ways for anonymous and pseudonymous communications online, and this is increasingly untraceable without significant multijurisdictional investigative efforts.

[162] See, for example, Data Protection Act 2018, ss 34 to 40.

Example 4

Marco and Roberto are two Italian computer science students and friends on an Erasmus year in England. Roberto has recently been accused of raping someone on their course, Jane Smith. Marco can't believe that this would have occurred. He was recently sent footage of Jane performing a striptease on a private messaging group called Telegram, which had apparently been sent to another student after the supposed rape. Marco thinks Jane has made up this rape story.

Marco decides he needs to help his friend and expose Jane for who she really is. He understands, however, that what he is about to do could get him in trouble, so he takes steps to "cover his tracks". First, he pays for an anonymous VPN service, that is based in Eastern Europe, using an anonymous cryptocurrency called "Monero". He then goes to a small internet café, and connects through the internet there to his VPN service. He uses his browser in "incognito mode" to search for an anonymous temporary email service. Once he has set up an account, he sends emails with the attachment of the striptease to a large number of university group email lists. He names the rape victim in the emails and adds a message stating "is this really what you'd do if you were raped a couple of days beforehand? Jane Smith is a liar and a slut".

The email is seen and read by many staff and students in the university. From there, it is further shared across numerous platforms, and file sharing Torrent sites like "Pornbay". The title for the video on the torrent site is "Jane Smith does striptease a day after a supposed rape". It quickly becomes a popular downloaded video on "Pornbay".

Analysis

10.161 Marco has undoubtedly committed a number of criminal offences in the United Kingdom, including under section 1 of the Sexual Offences (Amendment) Act 1992, and section 33 of the CJCA 2015.

10.162 He has published in England and Wales the name of the victim of a rape (Jane Smith) and a "moving picture" of her, thus jeopardising her anonymity.

10.163 He has also disclosed a private sexual video without her consent, and with an intention to cause distress.

10.164 Although he was routing his communications through an Eastern European server, these offences were committed in the United Kingdom, as a substantial proportion of the criminal behaviour occurred here.[163]

10.165 All of the individuals that have downloaded the video, and were seeding it to other users, may also have committed these offences in England and Wales, even if they

[163] See *R v Sheppard and Whittle* [2010] EWCA Crim 65; [2010] 1 WLR 2779.

were not physically in the jurisdiction when they downloaded and shared the video (explained further in Chapter 2).

10.166 However, Marco has taken a number of steps which would make it exceptionally challenging for law enforcement to find him. Police would need to begin by gathering communications data – if any were stored – from an anonymous email service provider, which is not based in the jurisdiction, and may or may not be responsive to police requests. They would then also need cooperation from the VPN service provider, who is again not in the jurisdiction. Once cybercrime investigations start to become this complicated, police are often forced to give up; they do not have the time, resources or legal powers to pursue the case.

10.167 Bringing actions against those that shared the videos using torrents may be possible, if their IP addresses were not otherwise masked, but this may again be a complex affair as the case of *AMP v Persons Unknown*[164] illustrates.

CONCLUSION

10.168 We have seen in this Chapter that there are a number of offences that might be charged in the context of sex-related privacy offences, most notably section 33 of the CJCA 2015. These are capable of prosecution where committed online, and in the case of the section 33 offence, largely designed for this context. However, many of the barriers to enforcement we have identified in other Chapters – such as cross-jurisdictional barriers and resourcing the prosecution of such a sheer scale of offending – are equally applicable to this offence.

10.169 In relation to the section 33 offence, there are definitional concerns around when a person might be said not to "consent" to the sharing of a private sexual image, and whether it might be appropriate to criminalise private image sharing which was intended primarily as a joke, rather than to cause distress. This is particularly so where the effect of that conduct is to cause the subject of the content serious distress.

10.170 These questions are not exclusively applicable to the online environment, although they are most likely to arise in this context.

10.171 We have also noted that technological advances in the production of altered imagery may mean that further consideration of the exclusion of these images from the scope of the offence is worthy of reconsideration.[165] Similar concerns were expressed very recently by the Women and Equalities Committee of the House of Commons of the House of Commons published its report into *Sexual harassment of women and girls in public places*.[166]

---

164 [2011] EWHC 3454 (TCC); [2011] Info TLR 25.

165 The government has announced it will ask the Law Commission to take forward a more detailed review of the law around the taking and sharing of non-consensual intimate images – see *Hansard* (HC), 5 September 2018, vol 646, col 282 (Lucy Frazer QC MP). At the time of the publication of this Scoping Report, the details of this review had not yet been confirmed.

166 Sexual harassment of women girls in public places, Report of the Women and Equalities Committee of the House of Commons (October 2018) HC 701, pp 19 and 20.

10.172 Our analysis also suggests that there is sometimes a lack of an effective criminal remedy in the context of "doxing" or "outing" conduct, with the offences under section 170 of the DPA 2018 carrying a maximum penalty of a fine only. Although other offences such as harassment or communications offences may apply in some cases, where they do not, many would consider DPA 2018 penalties to be inadequate in the most harmful cases.

10.173 For example, one can imagine circumstances where the widespread disclosure of personal information – such as a person's sexual history, or the fact they have a chronic disease – could have a devastating impact on their lives. In the worst cases – such as the Tyler Clementi and Tizia Cantone cases we have referred to in this Chapter – disclosure of private information could even drive a person to self-harm or suicide.

10.174 Breaches of personal privacy are not a new phenomenon, but the ease with which personal information can spread online, and the difficulty in suppressing or erasing such information once released, heightens the harm of privacy offending significantly.

10.175 An issue that we therefore consider worthy of further consideration is whether there is a need for more stringent penalties to punish and deter the most harmful privacy breaches.

Chapter 11: False communications

INTRODUCTION

11.1 This Chapter considers crimes which involve the communication of false or misleading information.

11.2 The online environment provides a fertile ground for the spread of false communications, and creates particular challenges for the criminal law in seeking to curtail the most serious conduct.

11.3 In this Chapter, we focus first on the offences contained in section 127(2) of the Communications Act 2003 ("CA 2003") and section 1 of the Malicious Communications Act 1988 ("MCA 1988").

11.4 These offences criminalise (amongst other things) the dissemination of false information with the intention of causing to another "distress or anxiety"[1] or "annoyance, inconvenience or needless anxiety".[2]

11.5 We also consider how other specific offences that relate to spreading false information operate in an online context, including:

- public safety offences: bomb hoaxes and false alarms of fire;
- public justice offences: perverting the course of justice, wasting police time and impersonating a police officer; and
- electoral offences: false statements as to election candidates.

11.6 We then look at conduct which is not subject to a specific criminal offence at present, including the abolished offence of criminal libel, and conduct that might be described as "identity theft", "catfishing" and "fake news".

11.7 We also briefly look at civil measures for regulating false or misleading communication online, including media regulation, self-regulation by social media platforms and the law of civil defamation. However, detailed consideration of these measures is beyond the scope of this project.

11.8 False statements made online can also amount to fraud.[3] Online fraud now accounts for one in six crimes. In 2016, it was estimated to cost individuals £10 billion, and the private sector £144 billion, in the UK.[4] There are also offences under consumer and

---

1 Malicious Communications Act 1988, s 1.

2 Communications Act 2003, s 127(2).

3 See Fraud Act 2006.

4 The Growing Threat of Online Fraud, Report of the Committee of Public Accounts (2017-19) HC 399, p 8. This data was originally sourced from: University of Portsmouth Centre for Counter Fraud Studies, *Annual*

business protection laws that prohibit false and misleading statements in the context of business and financial services.[5] However, online fraud and consumer protection are beyond the limited terms of reference for this review, and we do not consider them in this Chapter.

11.9 Our focus is on communication offences dealing with false or misleading information, committed online, where the purpose of the sender is to cause distress and upset to individuals. We also consider false communications which damage society more generally, such as offences that damage the democratic processes of government and the criminal justice system.

11.10 We conclude by noting the particular challenges posed by false communications offending in an online context, and provide examples to illustrate these.

FALSITY

11.11 Before considering the offences themselves, it is necessary to consider briefly what we mean by the concept of "falsity".

11.12 The offences we consider below all require a false communication to be made; that is, the expression of false or inaccurate information.

11.13 Whether or not a statement is in fact false is an objective question of fact for the tribunal to determine. Depending on the case, this may not always be clear. For example, in defamation law, the boundary between fact, honest opinion and falsehood has become increasingly blurred in the context of the proliferation of online customer reviews, where one person's "honest opinion" on their experience can be another person's defamatory falsehood.[6]

11.14 In each of the criminal offences we discuss, the tribunal must determine whether the defendant knew or believed the communication to be false.[7] This is a subjective question, and will require evidence as to the defendant's genuine belief as to the truth or falsity of the statement. For example, the offence of perpetrating a bomb hoax, considered further below, requires evidence that the defendant knows, or believes, that the statement that a bomb is present is a false statement. The separate offence of making a false statement as to an election candidate additionally requires proof that the defendant did not have "reasonable grounds" for their belief in the truth of their statement.

Fraud Indicator 2016 (May 2016), available at http://www2.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Annual-Fraud-Indicator-2016.pdf.

5 See Consumer Protection from Unfair Trading Regulations 2008, regs 9 and 10; Business Protection from Misleading Marketing Regulations 2008, pt 2; Financial Services Act 2012, pt 7.

6 See C Coors, "Opinion or defamation? Limits of free speech in online customer reviews in the digital era" (2015) 3 *Communications Law* 72.

7 This is in contrast to civil defamation, which is a strict liability tort, where there is no need to show the defendant knew the statement to be false. We discuss civil defamation in more detail at paras 11.98 to 11.108 below.

11.15 Each of the offences that we consider also requires that the defendant has a further intent – what criminal lawyers often call an ulterior intent – when sending the false message. In the case of the communications offences that is an intention to cause "distress or anxiety" [8] or "annoyance, inconvenience or needless anxiety";[9] while other offences require an intention to cause someone to form a belief of some kind (for example, that there is a bomb present at a location).

11.16 The offences do not rely on the more complex concept of "dishonesty", which underpins many fraud and theft offences, and has been the subject of recent judicial discussion.[10]

RELEVANT OFFENCES INVOLVING FALSE INFORMATION

Communications offences

11.17 We discuss the communications offences under section 127 of the CA 2003 and section 1 of the MCA 1988 in greater detail in Chapter 3. Below, we analyse their application in the specific context of false communications.

Section 127(2)(a) or (b) of the Communications Act 2003

11.18 Section 127(2) of the CA 2003 creates an offence of sending a "message that [D] knows to be false" by means of a public electronic communications network,[11] or causing such a message to be sent.[12]

11.19 Requiring the sender[13] to know that the message is false protects people who legitimately believed the information they were sending was true. In an online world, particularly with the proliferation of "fake news" across social media, there is a wide range of information disseminated across the internet which is, in fact, false but is commonly believed to be true.

11.20 The offence is only committed where the sender, or the person causing the message to be sent, knows that the message is false, and sends it "for the purpose of causing another person annoyance, inconvenience or needless anxiety".

11.21 A key term here is "another" person. According to the wording of the provision, the sender's intent does not necessarily have to be directed at the person to whom the false information relates, it could be directed at anyone who sees the message in question. Alternatively, the terms of section 127(2) indicate that the offence could also occur in circumstances where D sends false information to X with the purpose of annoying Y. In this scenario, the legislation appears to suggest that as long as D intended to annoy Y, D does not need to personally inform Y about sending the false information to X, for breach to have occurred. What precisely is meant by the terms "annoyance", "inconvenience" or "needless anxiety" is unclear, with little reported case law on the

---

8 Malicious Communications Act 1988, s 1.

9 Communications Act 2003, s 127(2).

10 See *R v Ghosh* [1982] QB 1053; *Ivey v Genting Casinos (UK) Ltd* [2017] UKSC 67; [2018] AC 391 at [74].

11 Communications Act 2003, s 127(2)(a).

12 Communications Act 2003, s 127(2)(b).

13 The definition of "sender" for the purposes of the Communications Act 2003 is discussed in Chapter 4.

matter. While it may guard against prosecution of every "white lie" that is sent via the internet, it still suggests a wide scope for the offence, particularly in an online context where it is easy to cause inconvenience to a very wide audience. It may protect those who intend to be humorous, however, in some cases there may also be the intent to inconvenience.

11.22 A recent example of a successful prosecution under this offence was the case of Stephen Dure, a self-styled "paedophile hunter", who was sentenced to 15 weeks' imprisonment for making false claims online that another man was a "violent psychopath" who "grooms teenagers".[14] The section 127(2) offence is a conduct crime, which means that it is committed even if no person actually receives the communication.[15] For example, if a disgruntled ex-partner were to send a message to the new partner of their ex, falsely claiming their ex had a sexually transmitted disease, this could potentially be an offence under section 127(2)(a), even if the recipient deleted the message before reading it. The fault element (the intention to cause annoyance, inconvenience or needless anxiety) might be proven without needing to show it actually did cause those harms. It also widens the application of the provision; a lot of false information (about celebrities, for example) is shared online but rarely reaches the person to whom it is targeted. As such, the "harm" element of this offence does not relate to the impact on a particular individual, but rather the harm to society at large of publishing false information that some may rely upon.

11.23 The maximum penalty for this offence is six months' imprisonment or a fine.[16]

11.24 Internal case management data provided by the Crown Prosecution Service ("CPS") indicates that 254 prosecutions of the section 127(2)(a) and (b) offences reached a first hearing at a magistrates' court in 2017.[17]

Section 1 of the Malicious Communications Act 1988

11.25 As noted in Chapter 4, section 1 of the MCA 1988 has its genesis in the Law Commission's 1985 report on Poison Pen Letters, which argued for the need to criminalise conduct that did not fall within existing offences, such as (the then applicable) offence of criminal libel.[18]

11.26 The behaviour criminalised by section 1(1)(a)(iii) of the MCA 1988 is any sending of "a letter, electronic communication or article of any description which conveys […] information which is false". Like section 127(2) of the CA 2003, this is quite a broad

---

14 See J Wood, *Paedophile hunter, 34, who carried out sting operations against alleged offenders is jailed for 15 weeks after falsely claiming innocent man groomed teenagers - causing him to lose his job* (4 September 2018), available at https://www.dailymail.co.uk/news/article-6129827/Paedophile-hunter-34-jailed-15-weeks-FALSELY-claiming-innocent-man-groomed-teenagers.html.

15 *DPP v Collins* [2006] UKHL 40; [2006] 1 WLR 2223 at [8].

16 Communications Act 2003, s 127(3).

17 Note that the CPS does not collect data that constitutes official statistics as defined in the Statistics and Registration Service Act 2007. These data have been drawn from the CPS's administrative IT system, which (as with any large scale recording system) is subject to possible errors with data entry and processing.

18 Poison Pen Letters (1985) Law Com No 147.

offence, where liability will often turn on establishing that the defendant had the requisite criminal purpose.

11.27 The fault element of the offence is that the defendant knows or believes the information they are sending is false, and one of their purposes is "to cause distress or anxiety to the recipient, or any other person to whom they intend its contents or nature should be communicated".[19] Of note, this provision differs from section 127(2) of the CA 2003, by requiring that the defendant acts with the purpose that the recipient – or intended viewer – of the communication, rather than just "another", is caused distress or anxiety.

11.28 Again, there is no requirement that the communication is actually seen by anyone for the offence to be committed.

11.29 An attempt may also suffice: for example, criminalising the defendant who believes he is sending a false statement if it is in fact true. Inchoate offences are discussed further in Chapter 12.

11.30 The maximum penalty for this offence is two years' imprisonment or a fine.[20]

11.31 A total of 2623 prosecutions were brought under section 1(1)(a) of the MCA 1988 in 2017. However, this figure was not further broken down between other variants of the offence (threats, indecency and gross offensiveness), which are likely to account for a sizeable proportion of these prosecutions.

Hoaxes and false alarms

Bomb hoaxes

11.32 A specific offence of creating a bomb hoax, punishable by a maximum penalty of seven years' imprisonment, exists under section 51 of the Criminal Law Act 1977.

11.33 The offence applies where a person "communicates any information which he knows or believes to be false to another person with the intention of inducing in him or any other person a false belief that a bomb or other thing liable to explode or ignite is present in any place or location".

11.34 The fault element of this offence is that the person knows or believes the information to be false, and intends to induce in someone else a false belief that a bomb or other thing is liable to explode.

11.35 It is not necessary for the defendant to specify the location of the bomb for the offence to be committed, nor is it necessary to show that the defendant had any particular target in mind with regard to the inducement of the belief.[21]

---

19 Malicious Communications Act 1988, s 1(1).

20 Malicious Communications Act 1988, s 1(4).

21 HHJ Thornton and others, *The Law of Public Order and Protest* (2010), p 65.

11.36 When sentencing for this offence, the courts have increasingly emphasised the need to deter this behaviour.[22] For example, in *R v Philipson* the Court of Appeal stated:

> the public and the emergency services require protection from those who potentially cause fear and disruption through bomb hoaxes, and that deterrence is of critical importance. It will be rare, if ever, that a bomb hoax offence will result in a non-custodial sentence, regardless of personal mitigation.[23]

11.37 It is possible that a bomb hoax may be committed online. For example, by tweeting "there is a bomb at Bloggs School, 1 Smith Street" the defendant could be found to have intended to induce in someone else a false belief that a bomb liable to explode.

Hoaxes involving noxious substances or things

11.38 It is also an offence under section 114(2) of the Anti-Terrorism, Crime and Security Act 2001 for a person to:

> communicate information which he knows or believes to be false with the intention of inducing in a person anywhere in the world a belief that a noxious substance or other noxious thing is likely to be present (whether at the time the information is communicated or later) in any place and thereby endanger human life or create a serious risk to human health.

11.39 The maximum penalty on indictment is seven years' imprisonment.[24]

11.40 A recent prosecution of this offence occurred after a man called Gatwick Airport to make a hoax bomb threat to ensure his flight – for which he was running late – was delayed. After pleading guilty to the section 114(2) offence, the man was sentenced to 10 months' imprisonment.[25]

False alarms of fire

11.41 An offence of giving a false alarm of fire exists under section 49(1) of the Fire and Rescue Services Act 2004.

11.42 The elements of the offence are that the defendant "knowingly gives or causes to be given a false alarm of fire to a person acting on behalf of a fire and rescue authority".

11.43 The offence is a summary offence with a maximum penalty of six months' imprisonment.[26]

---

22 HHJ Thornton and others, *The Law of Public Order and Protest* (2010), p 66.

23 *R v Philipson* [2008] EWCA Crim 1019; [2008] 2 Cr App R (S) 110 at [10].

24 Anti-Terrorism, Crime and Security Act 2001, s 114(3)(b).

25 M Busby, *Man jailed for making hoax bomb threat to avoid missing flight* (16 August 2018), available at https://www.theguardian.com/uk-news/2018/aug/16/man-jailed-for-making-hoax-bomb-threat-to-avoid-missing-flight.

26 Fire and Rescue Services Act 2004, s 49(2). Note that while the provision states that a maximum penalty of 51 weeks may be imposed, a magistrates' court does not have the power to impose a sentence of more than six months in respect of any one offence (see Powers of Criminal Courts (Sentencing) Act 2000, s

Administration of justice offences involving falsehood

Perverting the course of justice

11.44 The common law offence of perverting the course of justice is committed where one or more people commits an act or embarks on a course of conduct which has a tendency to, and is intended to, pervert the course of public justice.[27]

11.45 The "course of justice" refers to the use of criminal justice resources, such as processes of pre-investigation (between alleged conduct and investigation), investigation and trial (including aspects such as witnesses and the jury).

11.46 It carries a maximum penalty of life imprisonment, though Ministry of Justice statistics indicate that the average custodial length for the offence is approximately one year of imprisonment.

11.47 The case of *R v Rowell*[28] confirmed the principle laid out in *R v Vreones*[29] that the conduct must have both the tendency to pervert,[30] as well as an intention to pervert. Simply intending to pervert the course of justice is not sufficient to constitute an offence. However, it is not necessary for the risk to materialise in fact for the offence to be made out; an attempt would suffice (see Chapter 12).[31]

11.48 The offence covers a broad range of conduct, including falsifying or destroying evidence and intimidating witnesses. However, one of the most significant ways the offence can be committed is through the provision of false information, such as the making of false allegations, and the provision of false information to police.

11.49 In the case of false allegations, it is not necessary to show that the defendant intends the person to be arrested for the offence to be committed, merely that the defendant had the intention that the police would take the allegation seriously.[32] This offence is considered to be very serious. The courts have indicated that charges should only be pursued where there are significant aggravating features, such as wasting a great deal of police time and resources, or where innocent members of the public are falsely implicated and subject to questioning or detention.[33]

78(1)). Moreover, pursuant to the Fire and Rescue Services Act 2004, s 49(3), any section 49(1) offence committed before the commencement of Criminal Justice Act 2003, s 281(5) (which, as of 26 September 2018, was not yet in force), is to have a maximum imprisonment period of three months. As such, the maximum term of imprisonment is effectively three months.

27 *R v Vreones* [1891] 1 QB 360 p 369.

28 [1977] *Criminal Law Review* 681; [1978] 1 WLR 132.

29 [1891] 1 QB 360.

30 A "tendency to pervert" was confirmed in *R v Murray* [1982] 1 WLR 475 to mean that what the defendant has done, "without more", might lead to the incorrect result such as an innocent person being arrested.

31 *R v Murray* [1982] 1 WLR 475.

32 *R v Cotter and Others* [2002] EWCA Crim 1033; [2003] QB 951.

33 *R v Sookoo* [2002] EWCA Crim 800; *The Times* 10 April 2002 at [8].

11.50 When the offence of perverting the course of justice has been committed in a number of online contexts, it has been dealt with by the criminal law in a similar vein to offline acts.

11.51 For example, in the case of *R v Danevska*[34] in 2017, the defendant was convicted of two counts of perverting the course of justice, in addition to three offences of stalking, and sentenced to five years' imprisonment. In the course of stalking B, a man with whom she had developed an obsession, as well as P and M, two women who were in relationships with B, the defendant set up false email addresses and social media profiles in their names. She subsequently used these to send many threatening, abusive and malicious messages between them, and to their friends. The messages included information gleaned from her own observations of them, and gave the impression that the abusive messages were being sent by P and that P was the stalker. P was arrested as a result and kept in custody for a number of hours. The defendant then sent over 160 online police reports, disguising their origin, in 75 of which she made accusations that B was a rapist. She named B's colleagues as victims, witnesses or perpetrators. This led to a number of emergency police responses, wasting a significant amount of public resources. This is an example of how abusive online communication can be used to pervert the course of justice.

11.52 The *Danevska* case demonstrates the seriousness with which the common law offence may be perpetrated using online means, and the way that online communication can increase the scale of this type of offending. At the sentencing appeal of this case, the judge, in dismissing the appeal, also highlighted the abusive aspect of the crime. The judge took into account the mental anguish suffered by the victims, and noted that this psychological harm should not be viewed as less harmful than physical injury. Indeed, the defendant had caused significant harm to the victims' reputations, relationships and lives; at the height of her offending, they lived in constant fear of what the defendant would do next.

11.53 The CPS also recently announced that it is pursuing charges of perverting the course of justice against a man – known in the media as "Nick" – for allegedly sending the police emails from a fake account alleging that he had been raped and abused in the 1970s and 1980s by a number of powerful men.[35]

11.54 Given that messages on social media and other forms of online communication can be crucial evidence in cases (most notably, those involving sexual offences), deleting online communication can also constitute the offence of perverting the course of justice. There have, for example, been cases of victims selectively editing evidence of online messages that are used in the prosecution of other offences. Danny Kay spent more than three years in prison for rape, before a series of deleted messages between him and the complainant were uncovered and led to his conviction being quashed as unsafe.[36] Such conduct by a complainant could potentially amount to perverting the course of justice. However, given the complexity of sexual offence allegations, the CPS

---

34 [2017] EWCA Crim 1084.

35 Crown Prosecution Service, *Man charged with perverting the course of justice* (3 July 2018), available at https://www.cps.gov.uk/cps/news/man-charged-perverting-course-justice.

36 *R v Kay* [2017] EWCA Crim 2214; [2018] All ER (D) 38.

has strict guidance about the circumstances in which perverting the course of justice charges should be pursued.[37] No such charges have been pursued in the Kay case.

11.55 Destroying, falsifying or concealing potential evidence can occur even before legal proceedings have been instigated. An example of this is the case of *R v T*.[38] In 2011, T was convicted of perverting the course of justice for deleting indecent photographs of children found on a memory stick and shown to her by her daughter. T's husband had a previous conviction, and was imprisoned, for downloading indecent photographs of children from the internet. The Court concluded that T had deleted the photographs with the intention of preventing another investigation into her husband. While in this case the memory stick was not strictly an online source, T's husband had downloaded the photographs from the internet. This case demonstrates the ease with which perverting the course of justice can occur by deleting digital evidence that relates to online communication.

Wasting police time

11.56 An alternative, lesser charge to perverting the course of justice is the statutory offence of wasting police time, which carries a maximum penalty of six months' imprisonment.[39]

11.57 This offence is available where a person causes wasteful employment of the police by knowingly making a false report that an offence has been committed; or giving rise to apprehension for the safety of any persons or property; or that they have information material to any police inquiry.

11.58 The offence is available in a wider range of circumstances than perverting the course of justice, as it also covers circumstances such as false claims that a person is in danger.

11.59 Like perverting the course of justice, there is no reason why the offence of wasting police time could not be committed online. For example, false reports could be emailed to the police or sent to them by way of social media.

Impersonating a police officer

11.60 Where a person with intent to deceive impersonates a police officer, including through making a statement calculated to falsely suggest they are a police officer, they commit an offence under section 90 of the Police Act 1996, which carries a maximum penalty of six months' imprisonment.

11.61 It is possible that this offence could be committed online – for example, through establishing a false "ask a police officer" help website, or by creating a Facebook profile in the name of a police force. It is also arguably easier to commit this offence online than offline, as online impersonation does not require face-to-face interaction and

---

37 Crown Prosecution Service, *False Allegations of Rape and/or Domestic Abuse, see: Guidance for Charging Perverting the Course of Justice and Wasting Police Time in Cases involving Allegedly False Allegations of Rape and/or Domestic Abuse*, available at https://www.cps.gov.uk/legal-guidance/false-allegations-rape-andor-domestic-abuse-see-guidance-charging-perverting-course.

38 [2011] EWCA Crim 729.

39 Criminal Law Act 1967, s 5(2).

allows for access to a wider range of victims (particularly if the victim is estranged from the defendant, such as an ex-partner).

11.62 In 2017, for example, a woman who posed as a fake police officer online for more than two years to control her ex-boyfriend was convicted of impersonating a police office in addition to stalking charges, and sentenced to nine months' imprisonment. In addition to impersonating a police officer, she created fake witness accounts, and used these to manipulate the victim, dictating when he could go out, where he could go, and his social interaction with other people.[40]

False statements as to election candidates

11.63 It is an offence under section 106 of the Representation of the People Act 1983 to make or publish any false statement of fact in relation to the personal character of a candidate prior to or during an election.[41] This offence was reviewed in our Joint Consultation Paper on Electoral Law in 2014,[42] and subsequent Interim Report.[43]

11.64 The fault element of this offence is that the defendant has the purpose of affecting the outcome of the election, and does not believe, on reasonable grounds, that the statement is true.

11.65 To "make" or "publish" is not defined in the Act, which may pose difficulties in applying this offence in the online context. For example, using a similar approach to that under the Obscene Publications Act 1959, 'publish' would no doubt include a public tweet, but might not cover a private message, for example, via social media. Further, would a retweet constitute "publication" for the purposes of this Act? Would the term "make" cover these other online communications? The law is yet to answer these online-specific questions.

11.66 The primary justification for this offence, which has existed in some form since 1895, is to protect the integrity of the electoral process.[44]

11.67 Courts have emphasised that there is an important distinction between false statements about the political conduct of a candidate – criminalisation of which would very significantly curtail freedom of political debate – and false statements about the

---

40 BBC, *Shrewsbury stalker impersonating police jailed* (1 September 2017), available at https://www.bbc.co.uk/news/uk-england-shropshire-41128838.

41 For a fuller discussion of this and other electoral offences see Electoral Law: A Joint Consultation Paper (2014) Law Commission Consultation Paper No 218; Scottish Law Commission Discussion Paper No 158; Northern Ireland Law Commission No 20, Chapter 11, p 250.

42 Electoral Law: A Joint Consultation Paper (2014) Law Commission Consultation Paper No 218; Scottish Law Commission Discussion Paper No 158; Northern Ireland Law Commission No 20.

43 Electoral Law: An Interim Report (2016) Law Commission; Scottish Law Commission; Northern Ireland Law Commission.

44 J Rowbottom, "Lies, Manipulation and Elections—Controlling False Campaign Statements" (2012) 32(3) *Oxford Journal of Legal Studies* 507, p 510.

candidate's personal character. The latter are much harder for the public to adopt an informed view about, and might appropriately be subject to restriction.[45]

11.68 In the leading case of *Woolas*,[46] the High Court held that statements suggesting a candidate was wooing the extremist vote related to political conduct. In contrast, statements that a candidate was willing to condone threats of violence in pursuit of political advantage were found to be false statements about the candidate's personal character, and were therefore prohibited.[47]

11.69 There is also a distinct offence of knowingly publishing a false statement of a candidate's withdrawal at the election for the purpose of promoting or procuring the election of another candidate.[48]

11.70 Both of these offences are triable summarily and carry a maximum penalty of a fine.[49]

11.71 Additionally, these offences have the following electoral consequences:

(1) they vitiate the validity of an election if an election petition is brought;

(2) the offender is disqualified from election for a period of three years;[50] and

(3) if the offender is the winning candidate, he or she must vacate the elected post, and a new election must be held.[51]

11.72 Arrests have been made in relation to comments about candidates made on Facebook.[52]

Conduct which is not subject to a specific criminal offence

Criminal libel abolished in 2010

11.73 Prior to its abolition in 2010,[53] the common law offence of defamatory libel was available where a person had made untrue statements about another that were "so serious that

---

45 *R (on the application of Woolas) v The Parliamentary Election Court* [2010] EWHC 3169 (Admin); [2012] QB 1 at [109] to [124].

46 *R (on the application of Woolas) v The Parliamentary Election Court* [2010] EWHC 3169 (Admin); [2012] QB 1.

47 *R (on the application of Woolas) v The Parliamentary Election Court* [2010] EWHC 3169 (Admin); [2012] QB 1 at [121].

48 Representation of the People Act 1983, s 106(5).

49 Representation of the People Act 1983, s 169.

50 Representation of the People Act 1983, s 173(1)(b) read with s 173(4) to (8).

51 Representation of the People Act 1983, s 173(1)(a) read with s 173(2) and 173(3).

52 For eg, a man was arrested in Boston, Lincolnshire, in the lead up to the 2015 general election: BBC, Man arrested over Facebook election candidate comments (24 April 2015), available https://www.bbc.co.uk/news/uk-england-lincolnshire-32444069.

53 Coroners and Justice Act 2009, s 73(b).

it is proper for the criminal law to be invoked" and the public interest required the institution of criminal proceedings.[54] Such prosecutions were rare in practice.

11.74 The Law Commission first recommended a narrowing of criminal libel in 1985,[55] but no action was taken until the offence of criminal libel was repealed together with the offences of sedition and seditious libel and obscene libel in the Coroners and Justice Act 2009.[56]

11.75 Defamation is now solely a civil matter in England and Wales, although criminal libel remains in force in many other jurisdictions.

No general offence of "identity theft"

11.76 Another phenomenon that is commonly associated with false statements made in the online context, is broadly referred to as "identity theft". This refers to a range of conduct that involves the misuse of "identity" in some form, such as impersonating someone else, misuse of the personal data of another, or the creation of a false persona.

11.77 Participants in our stakeholders' experiences event shared their experiences of this form of abusive online communication. In domestic abuse contexts, for example, perpetrators sometimes engage in a form of identity theft by pretending to be the victim on social media, in order to isolate the real victim from family and friends. The harm that this type of conduct can cause is significant; from psychological harm, to reputational damage, and destroyed relationships.

11.78 However, as a way of describing the conduct in law, the term "theft" is somewhat problematic, as a person's entire identity cannot be stolen; rather, aspects of that identity are appropriated, which may then be used to perpetrate further crimes.[57] A more appropriate term may be the use of "impersonation", similar to the offence of impersonating a police officer. This better captures circumstances when someone takes over another person's Facebook account and purports to be that person, or when someone purports to be another through an online dating app.

11.79 Unlike some common law jurisdictions,[58] there is no general offence of identity theft in England and Wales. There are specific offences that relate to "identity documents" under the Identity Documents Act 2010,[59] but these do not extend to identity information more broadly.

---

54 *Goldsmith v Pressdram* [1976] 1 QB 83, p 88.

55 Report on Criminal Libel (1985) Law Com No 149.

56 Coroners and Justice Act 2009, s 73.

57 J Clough, *Principles of Cybercrime* (2nd ed, 2015) p 240.

58 The Canadian Criminal Code, for example, has specific offences of "identity theft" and "identity fraud". See: Criminal Code (RSC, 1985, c. C-46), ss 402, 403. Relevant offences also exist in Australia and the United States: see, eg Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act 2011 (Cth); Identity Theft and Assumption Deterrence Act of 1998 (US).

59 Identity Documents Act 2010, ss 6 to 8.

11.80 However, this is not to say that the conduct typically associated with "identity theft" will not be criminal for other reasons. For example, unauthorised access to data in a person's computer is an offence under section 1 of the Computer Misuse Act 1990. It is also an offence under section 170 of the Data Protection Act 2018 for a person knowingly or recklessly to obtain or disclose personal data without the consent of the data controller.[60] Where someone uses someone else's personal identifying information in order to make a gain or cause a loss to another, offences such as fraud by false representation will be committed.[61] It is also an offence for someone to sell or offer to sell personal data, where it has been knowingly or recklessly obtained without the consent of the data controller.[62]

11.81 These data protection offences will typically apply in situations where someone is impersonating another. However, they have been criticised for not carrying an adequate penalty and therefore not reflecting the harm that can be caused by such conduct. The offences in section 170 of the Data Protection Act 2018 carry only a fine.[63] We discuss privacy offences further in Chapter 10.

11.82 In certain circumstances, false displays of personal information online might amount to an offence of harassment. For example, in *S v DPP*[64] the image of a security guard for an animal-testing company was put on a website with text falsely implying that the security guard had been previously convicted of violence. The defendant who took the photo was convicted of causing harassment, alarm or distress contrary to section 4A of the Public Order Act 1986. Such behaviour could also form part of a "course of conduct" for the purposes of an offence under the Protection from Harassment Act 1997. We discuss harassment and stalking further in Chapter 8.

11.83 Many online platforms have policies and practices in place to prevent the false assumption of identity online. For example, Twitter has an "impersonation policy" which prohibits portraying another person in a "confusing or deceptive manner". However, "parody, commentary, or fan accounts" are permitted.[65] Consequences for breach of the policy include permanent suspension of the account.

No offence of "catfishing"

11.84 Similarly, there is no specific offence for the common online phenomenon of "catfishing". This term refers to situations in a romantic context, where a person creates a fake online persona for the purpose of duping another into thinking they are someone else. This is not uncommon in the context of dating websites, online dating apps or other social

---

60 It is also an offence under this section to procure the disclosure of personal data to another person without consent, and retain personal data without consent. We discuss this offence further in Chapter 10.

61 Fraud Act 2006, s 2.

62 Data Protection Act 2018, s 170(4) to (5).

63 Data Protection Act 2018, s 196(2).

64 [2008] EWHC 438 (Admin); [2008] 1 WLR 2847.

65 See Twitter, *Impersonation policy*, available at https://help.twitter.com/en/rules-and-policies/twitter-impersonation-policy/.

media.[66] As Gillespie notes, similar crimes of "romance fraud" are not a new phenomenon, but the proliferation of online dating sites has created new and highly effective forums to pursue this kind of behaviour.[67]

11.85 There is no definitive definition of "catfishing". However, its distinguishing feature, when compared with other forms of online anonymity (for example, displaying incorrect contact details) or the use of online aliases (for example, writing a "real" personal blog which is in fact impersonating a fictional character) is the intent to deceive a person romantically. This can be devastating for the target of such behaviour.[68]

11.86 While there is no specific offence that describes this conduct, catfishing behaviour can amount to an offence in other ways. It might form part of a course of conduct for the purpose of the offences of harassment or stalking (see Chapter 8). Alternatively, if catfishing is pursued for a financial benefit, it might amount to fraud.

11.87 Although harassment or stalking more accurately captures this kind of conduct, if the defendant has acted with the purpose of causing another anxiety or distress, then it might also be pursued under section 1 of the MCA 1988. If the false messages were sent to cause annoyance, inconvenience or needless anxiety then an offence under section 127(2) of the CA 2003 may have also been committed.

11.88 Using a fake profile on a social media website, in order to gain access to the data stored in another person's account, may also potentially constitute a computer misuse offence.[69]

11.89 An extreme example of the damage that can be caused by "catfishing" or impersonation was the case of Joanne Berry. Berry posed as a colleague on various sex websites, in order to arrange a revenge attack on her colleague. While pretending to be her colleague, Berry claimed she liked roleplay and encouraged men to engage in a rape role play scenario, and then provided the address of her colleague. One of these men entered the victim's house as instructed but was made suspicious by the victim's panic and did not follow through with the scenario. Berry was convicted of a number of charges including putting the victim in fear of violence, committing an offence of assault with the intent of committing a relevant sexual offence, common assault of the victim

---

66 See, eg C Wilson, *Should "catfishing" be made illegal?* (24 February 2017), available at https://www.bbc.co.uk/news/uk-39078201; E Flynn, *Who's behind the screen? What does the phrase catfishing mean, and what's the law on stealing someone's identity online in the UK?* (19 September 2018), available at https://www.thesun.co.uk/fabulous/1754196/catfishing-meaning-identity-steal-online-dating/.

67 See A Gillespie, "The (electronic) Spanish Prisoner: Romance Frauds on the Internet" (2017) 81 *Journal of Criminal Law* 217.

68 The serious consequences of "catfishing" behaviour, and the importance of protecting victims, was recently explored in a parliamentary debate entitled "Catfishing and Social Media": *Hansard* (HC), 18 July 2017, vol 627, col 274WH.

69 For discussion see M Ó Floinn and D Ormerod, "Social networking sites, RIPA, and criminal investigations" [2011] *Criminal Law Review* 766, pp 771 to 774.

and attempting to cause the victim to engage in penetrative sexual activity without consent. She was sentenced to six years' imprisonment.[70]

No offence of "fake news"

11.90 Concern about the propagation of "fake news" and its potentially damaging effects has been particularly acute in recent years. The rise of non-traditional media and social media have been seen as the key drivers of this phenomenon.[71]

11.91 Online communication has allowed unqualified people to take on the role of "journalist" and spread inaccurate and uncorroborated information, for example, in the form of blogs and so-called "news" websites. Whereas traditional media sources generally conform to recognised journalistic standards, there is far less oversight in the accuracy of new media sources such as blogs, social media accounts and YouTube channels. Other users of online communication often take these sites at face value, which can contribute to the spreading of fake news throughout the internet. Moreover, a recent study, performed by academics at Yale University, has suggested that "prior exposure" to fake news stories – via social media – makes it more likely for people to believe disinformation spread through fake news.[72] It was identified that "fake-news credulity compounds with increasing exposures and maintains over time".[73]

11.92 The issue of fake news is currently the subject of an inquiry by the Digital, Culture, Media and Sport Committee of the House of Commons. It recently released an interim report outlining the particular damage that disinformation and fake news can cause to the proper functioning of democratic processes.[74]

11.93 A recent example of damaging fake news was the circulation of a picture of a woman wearing a hijab talking on the telephone on Westminster Bridge, following the terror attack there in March 2017. The image suggested that as a Muslim, the woman was indifferent to the suffering of victims around her and BanIslam was one hashtag circulating with the image. The woman subsequently released a statement, outlining her shock and the ways which she had sought to assist at the scene, which was supported by the photographer.[75]

---

70 Kent Online, *Joanne Berry jailed for six years for 'bizarre' rape revenge plot against Medway woman* (8 August 2014), available at http://www.kentonline.co.uk/medway/news/deranged-woman-jailed-over-rape-21626/.

71 See, eg T McGonagle, "'Fake news': False fears or real concerns?" (2017) 35(4) *Netherlands Quarterly of Human Rights* 203.

72 G Pennycook, TD Cannon and DG Rand, "Prior Exposure Increases Perceived Accuracy of Fake News" (2018) *Journal of Experimental Psychology: General* 1, p 2.

73 G Pennycook, TD Cannon and DG Rand, "Prior Exposure Increases Perceived Accuracy of Fake News" (2018) *Journal of Experimental Psychology: General* 1, p 10.

74 Disinformation and 'fake news': Interim Report, Report of the Digital, Culture, Media and Sport Committee (2017-19) HC 363, available at https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

75 TellMAMA, *The truth behind the photo of the Muslim woman on Westminster Bridge* (24 March 2017), available at https://tellmamauk.org/the-truth-behind-the-photo-of-the-muslim-woman-on-westminster-bridge/.

11.94 There is currently no general criminal offence of creating or spreading fake news in England and Wales.[76]

11.95 As noted above, there are specific offences that might be pursued in the context of an election campaign. However, in general, the law has avoided criminalising the spread of information purely on the basis that it is false, unless it is connected to fraud, or a misleading or deceptive trade practice.

11.96 The proposals of the Digital, Culture, Media and Sport Committee are focused on more effective regulation of the online environment, rather than new criminal offences.

11.97 To the extent that remedies exist for "fake news", they are primarily civil, through civil defamation proceedings and media regulation.

Civil remedies: defamation

11.98 The most important civil remedy available for the communication of false information is the tort of defamation. It exists primarily at common law, although it was substantially reformed by the Defamation Act 2013.

11.99 Defamation is an umbrella term encompassing the torts of libel and slander.[77] It provides a civil law remedy against a person who publishes a statement to a third party, that contains false information about an individual or organisation, which serves to undermine their reputation.[78] "Statement" is defined in section 15 of the Defamation Act 2013 as "words, pictures, visual images, gestures or any other method of signifying meaning".[79]

11.100 In general terms, libel refers to a publication that is permanent, broadcast, or part of a live theatre performance. Slander refers to more temporary publication. The statement must be "published" to a person other than the person who is being defamed by the statement.

11.101 In *McAlpine v Bercow*,[80] the Court had to consider the application of the Defamation Act 2013 to a social media post. In this case, the claimant had been a politician who had unfounded allegations of child sexual abuse made against him. The defendant had tweeted (on her Twitter account with 56,000 followers) "why is Lord McAlpine trending? *innocent face*". The Court found the words to be defamatory by innuendo.

---

76 However, note that section 127 of the Communications Act 2003 and section 1 of the Malicious Communications Act 1988 are potential sources of criminalisation, should the "spreading" of fake news involve "sending".

77 R Parkes and others, *Gatley on Libel and Slander* (12th ed, 2017) Chapter 1 at 1.5.

78 R Parkes and others, *Gatley on Libel and Slander* (12th ed, 2017) Chapter 1 at 1.4.

79 Defamation Act 2013, s 15.

80 *Lord McAlpine of West Green v Bercow* [2013] EWHC 1342 (QB).

11.102 In order for a statement to be defamatory, it must cause or be likely to cause "serious harm"[81] to the reputation of the claimant, a statutory test that was considered extensively by the Court of Appeal in *Lachaux v Independent Print Ltd*.[82]

11.103 Defamation is a tort of strict liability, whereby the impact of the publication is the primary element. It is not relevant whether the statement was published with malice, or conversely in good faith (but note the defences of honest opinion and public interest below).[83]

11.104 The main defences available to a defendant in a defamation proceeding are:

(1) truth: the statement that was made is true;[84]

(2) honest opinion: where an opinion held by the defendant was expressed and an honest person could have held the opinion on the basis of any fact that existed when the statement was published, or anything asserted to be a fact in a privileged statement;[85]

(3) privilege: comments made in parliament and under oath in court proceedings have absolute protection from defamation, while reports of parliament and court proceedings are also protected where fair and accurate;[86] and

(4) public interest: the statement complained of was, or formed part of, a statement on a matter of public interest, and the defendant reasonably believed that publishing the statement was in the public interest.[87]

11.105 A defendant may also make an "offer of amends" as an alternative resolution to the tort of defamation. If this offer is refused, the defendant has a defence to the claim, unless it can be demonstrated that he had reason to believe the words published about the claimant were false and defamatory.[88]

11.106 The Defamation Act 2013 also introduced a new defence for website operators who did not post the defamatory content on the website themselves.[89] Even where the

---

81 Defamation Act 2013, s 1.

82 [2017] EWCA Civ 1334; [2018] QB 594.

83 A tort of defamation has still occurred even if the defendant believed the words to be true: *Campbell v Spottiswoode* (1863) 3 B & S 769.

84 Defamation Act 2013, s 2. This statutory defence replaced the common law defence of "justification".

85 Defamation Act 2013, s 3. This statutory defence replaced the common law defence of "fair comment".

86 Privilege may be absolute or qualified; for further discussion, see R Parkes and others, *Gatley on Libel and Slander* (12th ed, 2017) Chapter 13 and Chapter 14.

87 Defamation Act 2013, s 4.

88 See: A Zuckerman, *Zuckerman on Civil Procedure: Principles of Practice* (3rd ed, 2013) Chapter 26.

89 Defamation Act 2013, s 5. Publisher defences under section 1 of the Defamation Act 1996 also remain in force. The court has grappled with the question as to whether certain web content providers are editors, publishers or a third party; eg, the liability of bloggers were considered in *Kasche v Gray* [2010] EWHC 690 (QB); [2011] 1 WLR 452; see also *England and Wales Cricket Board Ltd v Tixdaq Ltd* [2016] EWHC 575 (Ch); [2016] Business Law Reports 641 and *Tamiz v Google Inc* [2012] EWHC 449 (QB); [2012]

operator moderates statements on the website, this does not necessarily defeat the defence.[90] However, the defence will be defeated if the operator acted with malice.[91] To receive the benefit of the defence, websites must comply with the Notice of Complaint procedure set out in the Defamation (Operators of Websites) Regulations 2013.[92]

11.107 There are also protections available under the Electronic Commerce (EC Directive) Regulations 2002[93] in circumstances where providers act as a "mere conduit", "cache" or "host" of information.[94]

11.108 Detailed consideration of civil defamation law and platform liability is beyond the scope of this project; however, it provides some context as to how false statements are dealt with in other areas of the law.

Media regulation

11.109 Another key deterrent against the communication of false information is regulation and self-regulation of the media.

11.110 The regulatory environment for the print media in the United Kingdom is currently in a state of flux, but two main self-regulatory bodies currently exist: the Independent Monitor for the Press ("IMPRESS") and the Independent Press Standards Organisation ("IPSO"). Both of these organisations have established editorial codes which set out the importance of accuracy in reporting.[95]

11.111 Broadcast media organisations are regulated by Ofcom, which publishes the Ofcom Broadcasting Code. This Code emphasises the need for "due accuracy and due impartiality".[96]

11.112 There is inevitably a limit to the resources of each of these regulators; and it is not possible for them to act as ultimate arbiters of truth in the reporting of all cases. However, they can consider the investigative process of the media organisation, and how defensible their claims were based on the evidence before them.

Entertainment and Media Law Reports 24, the latter of which found that Google could not be considered a publisher for the purposes of a libel claim.

90 Defamation Act 2013, s 5(12).

91 Defamation Act 2013, s 5(11).

92 SI 2013 No 3028.

93 SI 2002 No 2013.

94 See the Electronic Commerce (EC Directive) Regulations 2002, SI 2002 No 2013, regs 17 to 19.

95 See Independent Press Standards Organisation, *Editors' Code of Practice*, available at https://www.ipso.co.uk/editors-code-of-practice/; and Editors' Code of Practice Committee, *The Editors' Codebook: The Handbook to the Editors' Code of Practice* (2018), available at http://www.editorscode.org.uk/downloads/codebook/codebook-2018.pdf; see also D Carney, "Up to standard? A critique of IPSO's Editor's Code of Practice and IMPRESS's Standards Code: Part 1" (2017) *Communications Law* 22(3).

96 Ofcom, *The Ofcom Broadcasting Code* (April 2017), available at https://www.ofcom.org.uk/__data/assets/pdf_file/0005/100103/broadcast-code-april-2017.pdf.

11.113 It is also important to note that these organisations only regulate established media organisations. IPSO, for example, refers to itself as the "independent regulator for the newspaper and magazine industry in the UK".[97] This is distinct from content created and published by individuals – in the form of bloggers, for example – or interest groups, who may create a website or social media page with information about their particular interest, that are not newspapers or magazines. In an era where a huge amount of content is created by private individuals or interest groups, the ability to ensure accurate reporting in the online sphere is limited.

11.114 Large social media platforms such as Facebook have taken some steps towards greater regulation of false content. Facebook's Community Standards state that while it will not remove false news that is posted on Facebook, it will seek to reduce its distribution by showing it lower in the News Feed.[98] Facebook has also now committed to deleting inaccurate or misleading information created or shared "with the purpose of contributing to or exacerbating violence or physical harm".[99]

11.115 Issues to do with regulation and self-regulation of the media and online environment are beyond the scope of this review, but provide important context in understanding what content is allowed to be published online.

FALSE COMMUNICATION AND FREEDOM OF EXPRESSION

11.116 As with all prosecutions, the exercise of the CPS' prosecutorial discretion for communications offences is subject to two key tests. An evidential test asks – is there enough evidence to convict? In addition, the CPS must consider whether it is in the public interest for the CPS to bring the case to court.[100]

11.117 The public interest test is particularly pertinent in communications offences, where prosecutors need to balance protection of the individual and the public, against the broader public interest in freedom of speech. The offences referred to in this Chapter – and in particular, the communications offences – engage Article 10 of the European Convention on Human Rights ("ECHR"), which protects the right to freedom of expression.

11.118 Article 10 protects not only speech which is well-received and popular, but also speech which is offensive, shocking or disturbing.[101] However, Article 10(2) states that the right:

---

97 Independent Press Standards Organisation, What we do, available at https://www.ipso.co.uk/what-we-do/; a list of who IPSO regulates can be found at Independent Press Standards Organisation, *UK Regulated publications*, https://ipso.co.uk/complain/who-ipso-regulates/.

98 See Facebook's Community Standards, *18: False news*, available at https://en-gb.facebook.com/communitystandards/integrity_authenticity/false_news.

99 O Solon, *Facebook's plan to kill dangerous fake news is ambitious – and perhaps impossible* (20 July 2018), available at https://www.theguardian.com/technology/2018/jul/19/facebook-fake-news-violence-moderation-plan.

100 See Crown Prosecution Service, *The Code for Crown Prosecutors* (January 2013), available at https://www.cps.gov.uk/sites/default/files/documents/publications/code_2013_accessible_english.pdf.

101 *Sunday Times v UK (No 2)* [1992] 14 EHRR 123.

may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, 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.

11.119 The European Court of Human Rights has held that Article 10 does not prohibit discussion or dissemination of information received, even if it is strongly suspected that this information might not be truthful. In *Salov v Ukraine*,[102] it held that to suggest otherwise would deprive persons of the right to express their views and opinions about statements made in the mass media, and would therefore place an unreasonable restriction on the freedom of expression set out in Article 10.[103]

11.120 As we have seen, bomb hoaxes,[104] justice offences, and election campaigns are three areas where parliament has placed limits on the right of freedom of expression, and criminalised the spread of false information. But CPS guidance urges prosecutors to exercise "considerable caution before bringing charges under section 1 of the MCA 1988 and section 127 of the CA 2003 due to the 'potential for a chilling effect on free speech'".[105]

11.121 This restraint means that communications offences often exist in a middle space; between conduct considered too low level to be worthy of prosecution, and conduct that amounts to other, more serious offences such as stalking and harassment.

ONLINE CONSIDERATIONS

11.122 Below, we consider examples that illustrate some of the challenges the online world presents for combatting offences involving false communication, which we have grouped under the following categories:

(1) Jurisdictional difficulties: propagation of false content created in foreign jurisdictions is sometimes beyond the reach of domestic criminal law.

(2) The scale of potential harm caused by online falsity: the 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.

---

102 (2007) 45 EHRR 51.

103 *Salov v Ukraine* (2007) 45 EHRR 51; Further discussion can be found in J Kleijssen's speech to The Royal Netherlands Society of International Law (KNVIR) *Spring meeting: Fake News and National Sovereignty* (13 June 2017), available at https://www.coe.int/en/web/human-rights-rule-of-law/jan-kleijssen/speech-the-hague-2017-06-13.

104 Though not where the hoax is clearly a joke, with no intention to induce a belief in others, see *Chambers v DPP* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833.

105 Crown Prosecution Service, *Social Media: Guidelines on prosecuting cases involving communications sent via social media* (2018), available at https://www.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media.

(3) Ease of commission: conversely, the communications offences, as currently in force, are very broad, and in some contexts may (at least theoretically) criminalise conduct which falls well short of what many consider worthy of criminal sanction.[106]

(4) Consistency of the criminal law offline and online: in some contexts, such as prank and stunt videos, the law currently operates in such a way that the relevant criminal conduct is only committed online, or only committed offline, which can seem anomalous. We illustrate this with two examples.

11.123 In addition, and consistent with most other offence areas we consider in this Report, the sheer volume of false content distributed online presents an enormous challenge for law enforcement. This is most obvious in the case of online fraud, where only a small fraction of incidents of offending each year are ever prosecuted. But it is equally true in other contexts. For example, the amount of untrue content disseminated for the purposes of inconveniencing or distressing another online is also likely to be vast. If all of this conduct, or even a small proportion of it, were to be prosecuted as one of the two applicable communications offences discussed above, the resourcing implications for the criminal justice system would be unmanageable.

Jurisdictional difficulties

11.124 We have seen that there are some key areas where the law already criminalises false communications, and this applies equally whether the conduct is committed online or offline. However, the global reach of the internet can mean that it is, in practice, impossible to enforce the criminal laws of England and Wales. For example, the perpetrators may be operating abroad, and even in a jurisdiction in which it is not a criminal offence to publish such material online.

[106] See J Rowbottom, "To rant, vent and converse: Protecting low level digital speech" (2012) 71 *Cambridge Law Journal* 355.

Example 1 – offending behaviour occurs beyond reach of law enforcement

Priya is a popular independent candidate running to become MP for a rural constituency in England. She has campaigned strongly for the preservation of the English countryside, and also on her conservative family values. She opposes the development of a major windfarm that is to be built and financed by a foreign corporation in Asia.

Priya is married with three children, and has made her family life a feature of the campaign.

During the campaign, numerous articles are published on social media falsely alleging that Priya has had an extra-marital affair.

The allegations are not picked up by the mainstream media as they are not independently verified, but they are widely read in the constituency, and beyond, on social media. Priya's polling numbers immediately drop significantly.

An investigation reveals that the source of these articles is someone based in the country where the windfarm company is located. It is strongly suspected that interests behind the windfarm venture are responsible for spreading the false allegations.

Analysis

11.125 A violation of section 106 of the Representation of the People Act 1983 may have occurred.

11.126 It is possible, following the principle in *R v Sheppard*,[107] (discussed further in Chapter 2) that a court might find that a "substantial measure" of the activities took place within the jurisdiction. However, in *Sheppard* an important factor was that the defendant uploaded in the United Kingdom, and the material was downloaded in the United Kingdom this hypothetical case would stretch that principle considerably.

11.127 In practice, it is also likely to prove very difficult to hold perpetrators in a foreign jurisdiction to account for such conduct, particularly if it is not a jurisdiction that has adequate extradition arrangements with the United Kingdom. Even if such arrangements were in place, it is unlikely that these offences would be considered of sufficient gravity to justify extradition proceedings.

11.128 This illustrates the limitations of domestic criminal law as a means of deterring and punishing online behaviour in a globalised environment.

[107] [2010] EWCA Crim 65; [2010] 1 WLR 2779.

Scale of harm

11.129 Freedom of expression is a fundamental component of modern democratic societies, and it is protected by Article 10 of the European Convention on Human Rights. However, the internet is now facilitating the exchange of information on a scale unprecedented in human history. While much of this knowledge exchange is positive, there can be examples where the spread of false information causes widespread harm in a manner that was not previously achievable.

Example 2 – wellness blogging

Ryan is a prominent 'wellness' blogger with more than 200,000 followers in England and Wales. He writes regularly about the importance of diet to health. While many of his claims are considered unscientific, his promotion of a generally healthy diet is considered largely benign by the medical community.

He shuns advertising and does not receive any form of remuneration for blogging, which enhances his credibility amongst his readership.

Recently, Ryan has been reading about the benefits of "high acid diets". He has become convinced by claims in the alternative wellness community overseas that an acidic diet is the only effective way to treat diabetes, and that traditional forms of treatment such as insulin are damaging and should be avoided.

Ryan writes persuasively on the topic, and despite warnings from medical professionals and the NHS, many readers with diabetes decide to shun traditional medicine in favour of his diet-based alternative.

In the ensuing two years, it is estimated that 12 people with manageable diabetes die unnecessarily as a result of following Ryan's advice.

Analysis

11.130 This example illustrates the scale of the potential dangers posed by false communications in the online environment. It might be arguable that Ryan had a duty of care to his readers for the purposes of gross negligence manslaughter.[108] However, given he is simply an advice blogger, it may also be difficult to establish the relevant duty.

11.131 Before the advent of mass communication over the internet, it would have been much harder for Ryan to reach such an audience, and cause harm on this scale. Had he

[108] See, eg Bernard Rebelo who was convicted of manslaughter at Inner London Crown Court, after selling the industrial chemical, "2, 4, dinitrophenol" (DNP) online for human consumption, after marketing it as a "slimming aid". A 21-year-old student, Eloise Parry, died in 2015 from the effects of taking the substance: Harrow Council, *Harrow Council wins landmark DNP manslaughter case* (27 June 2018), available at http://www.harrow.gov.uk/news/article/673/harrow_council_wins_landmark_dnp_manslaughter_case.

sought to spread such claims through traditional print and broadcast media, it would almost certainly have failed to meet editorial standards.

11.132 This raises a legitimate question as to whether there are certain contexts where the criminal law might rethink its reluctance to criminalise false claims outside traditional contexts such as fraud, consumer protection and the administration of justice.

11.133 At present, the Cancer Act 1938 prohibits advertising cancer treatments to the general public (whether or not they are effective),[109] and EU Regulations restrict the making of false nutrition and health claims in a commercial context.[110] However, there is no broader prohibition on the dissemination of false health information by members of the public.

11.134 Previously, such false health claims might have been tolerated on the basis of a broader commitment to freedom of expression. Could it now be argued that the potential harm caused by such conduct is so great that it justifies criminalisation?

Ease of commission

11.135 While the above example indicates the reluctance of the law to intervene in certain contexts, the false communication offences can (at least theoretically) be committed in contexts that might seem surprising.

11.136 The offence under section 127(2)(a) and (b) of the CA 2003 is particularly broad, as it may be committed simply where the intention is to cause another person "inconvenience". This means that many hoaxes and "April fools" jokes posted online could technically fall within the offence if the intention is to cause "inconvenience" to another.

11.137 It might also capture fairly low-level, petty behaviour between acquaintances or ex-partners, that would not be criminal if committed in person.

---

[109] Cancer Act 1938, s 4.

[110] See Council Regulation (EC) No 1924/2006 of 20 December 2006, regarding nutrition and health claims made on foods.

Example 3: post break up pettiness – could it be a criminal offence?

Amy and Thao have recently separated after a six-month relationship. Thao ended the relationship, leaving Amy angry and hurt. However, Amy knows Thao has a jealous streak, and seeks to get back at him.

Thao still follows Amy on Instagram, a photo sharing platform, and with the intention of upsetting Thao, Amy decides to post a series of false images and captions depicting a new relationship with a handsome fictional man named "Josh".

The captions state things like: "so in love with my man" and "when you decide to ditch the old model and upgrade to a real man".

Thao sees these images and is devastated.

Analysis

11.138 A degree of petty and irrational behaviour between ex-partners is not unusual, and unless it amounts to harassment of some kind (see Chapter 8), it is not normally conduct which involves the criminal law.

11.139 However, on a strict reading, Amy has arguably committed offences under both section 1 of the MCA 1988 and section 127(2) of the CA 2003, referred to above. This is because she has sent a false communication with the purpose of causing "distress or anxiety"[111] or "needless anxiety"[112] to Thao.

11.140 It is not even necessary for Thao to have seen or been upset by the posts for Amy to commit one of these offences; as these are conduct crimes it is sufficient that Amy sent the false communications with the requisite intention.

11.141 Had Amy made these same false claims and showed the photos to Thao in person, there would be no potential criminal offence whatsoever.

11.142 In practice, it is clear that the police would not investigate such a charge, and it clearly falls well short of the public interest test for the purposes of the CPS' charging discretion.

11.143 However, the example illustrates just how broadly the current communication offences apply in the context of false communications, and the huge array of conduct that is potentially drawn in.

---

111 Malicious Communications Act 1988, s 1.

112 Communications Act 2003, s 127(2).

Consistency of criminal law offline and online

11.144 The phenomenon of YouTube pranks and stunts, and their potentially deadly consequences, has become more prominent recently.[113]

11.145 For the purposes of false communication offences, the perspective of the audience can be significant in considering whether an online offence has been committed, as the following examples illustrate.

Example 4 – Facebook Live prank leading to panic at a shopping centre

Chris is a popular social media celebrity comedian, who works across several platforms including Youtube, Twitter and Facebook.

He has recently embarked on a series of "Facebook Live" pranking stunts, which typically have tens of thousands of viewers.

In one recent stunt, he decided to dress up in an over the top "terrorist" outfit, with fake bombs strapped to his chest, and ran through a busy shopping centre.

Chris's actions caused panic, and a number of people were seriously injured in a crush at the centre's exits.

Analysis

11.146 It is likely that Chris has committed a number of offences due to his physical conduct at the shopping centre, including threatening behaviour causing fear of provocation of violence, contrary to section 4 of the Public Order Act.[114]

11.147 However, the online component of his offending – the dissemination of the prank through Facebook Live – is unlikely to amount to an offence in its own right. This is because in relation to his viewers, Chris's intention is to provide humour (however misguided), rather than cause distress, annoyance, inconvenience or anxiety. He also has not committed a bomb hoax offence online, as again, he lacks the intention to induce a false belief in his viewers, who are "in" on the joke from the outset.

11.148 Conduct such as Chris's is not uncommon, with a large number of YouTube pranksters having caused serious harm in the physical world. But while the online environment may provide the motivation for the offence, it is not the forum on which the offence is actually committed.

---

113 A tragic example was the death of a young man in the United States after he asked his girlfriend to shoot a gun at him through a book, wrongly believing the book would stop the bullet. See T Marco, *Woman fatally shoots boyfriend in YouTube stunt* (29 June 2017), available at https://edition.cnn.com/2017/06/29/us/fatal-youtube-stunt/index.html.

114 The offence of public nuisance may be available in this context, however, given the judgment in *R v Rimmington* [2005] UKHL 64; [2006] 1 AC 459 at [38], the statutory offence under section 4 of the Public Order Act 1986 is more likely to be considered. For further discussion, see Chapter 8.

Example 5: faked shooting on Periscope

Naomi has a Periscope account, and decides that to increase her audience size she will shock them by filming a prank where her friend pretends to shoot her live on camera.

She has a background working in film and is quite skilled at making the shooting appear realistic.

She and her friend carry through the prank, and Naomi collapses to the ground, apparently dead. Her audience is indeed shocked, and many become distressed and call the police.

Analysis

11.149 By broadcasting the prank, Naomi has arguably committed an offence contrary to section 127(2) of the CA 2003. The video itself is not false in that it is a true recording of what occurred, but the way she is presenting the video – to pretend falsely she has been shot dead – is capable of amounting to an intention to cause the viewers "needless anxiety" for the purposes of the offence.

11.150 Interestingly, had she performed the same act in front of a live audience, she would not have contravened section 127(2) of the CA 2003. Alternatively, in such circumstances, Naomi may have breached section 5 of the Public Order Act 1986, should the behaviour be deemed disorderly – as people were likely to be caused alarm or distress. This is therefore an example of where an offence that is criminal online connotes a different offence offline.

CONCLUSION

11.151 False communications are one of the areas we consider in this Report where conduct committed online might amount to an offence in circumstances where no offence would be committed by equivalent conduct offline. The wording of section 127(2)(a) and (b) of the CA 2003, "annoyance, inconvenience or needless anxiety", and section 1 of the MCA 1988, "distress or anxiety", potentially criminalises a large volume of online communication.

11.152 In practice, the CPS prioritise prosecutions by applying rigorous charging guidelines to the prosecution of communications offences, and carefully weighs the seriousness of the offending against the right to freedom of expression. However, this approach places a large emphasis on prosecutorial discretion and it would arguably be more desirable for the law to provide certainty to online users.

11.153 One area which we therefore consider worthy of further consideration is whether the scope of the false communication offences should be drafted in such a way that can sensibly address the exponential growth in this type of online communication. For example, they could become "result" crimes, where some demonstrable harm is required in order for the offence to be committed. Alternatively, consideration could be

given to replacing words such as “annoyance” and “inconvenience” with higher thresholds such as “serious distress”.

11.154 This is not to say that harmful false communications should be decriminalised altogether, but the way the law is currently framed is arguably over-inclusive, potentially chilling freedom of expression and distracting law enforcement from pursuing the most serious offending.

11.155 Conversely, in this Chapter, we have also noted that there are some contexts in which the spread of false information, even where not done maliciously, may present serious risks to public health and safety. The spread of dangerously false health claims is one potential area we have identified. Dangerously false advice in other contexts – such as DIY home electrical maintenance – is potentially another. We therefore consider that this might be a matter for further consideration, given the scale of harm that is now possible in the online environment.

Chapter 12: Encouraging crime and other inchoate offences online

INTRODUCTION

12.1 In this Chapter we consider the law governing inchoate offences in the context of abusive and offensive online communications. "Inchoate" means just begun, incipient; in an initial or early stage.[1]

12.2 The basis of liability in inchoate offences centres on the defendant's blameworthy state of mind, although in every case some physical conduct by the defendant is also required before criminal liability can be imposed.[2] "Inchoate" criminal liability may exist notwithstanding that no tangible harm has occurred even where the full offence may require proof of that harm. For example, an offence of harassment requires proof that the victim suffered harassment, alarm or distress, but a conspiracy to cause harassment is committed irrespective of whether that harm arises. Liability for conspiracy is dependent on whether the six elements of the offence of statutory conspiracy have been satisfied.[3]

12.3 There are three main types of inchoate offences:

(1) conspiracies; where two or more people agree that a course of criminal conduct should be embarked upon;

(2) attempts; where a person does an act which is more than merely preparatory to the commission of the offence with the intent to commit the offence; and

(3) encouraging or assisting the commission of a criminal offence.

12.4 Inchoate liability depends on the existence of a substantive offence. The defendant becomes criminally liable for conspiring or attempting to commit, or encouraging the commission of, a substantive offence. A person cannot be criminally liable for attempting to commit an act that is not of itself criminal. However, the substantive offence does not actually need to be committed for inchoate liability to arise. For example, a person may be guilty of encouraging others to commit the offence of riot.[4] The person who did the encouraging can be liable even if he or she played no part in the riot itself, or the riot did not take place.

12.5 There are also offences known as "substantive inchoate offences", where the substantive offence itself takes the form of an inchoate offence. For example, the offence of assisting or encouraging suicide is an offence in its own right under sections 2 and

---

1 See D Ormerod and K Laird, *Smith, Hogan and Ormerod's Criminal Law* (15th ed, 2018) p 410.

2 G Yaffe, *Attempts: In the Philosophy of Action and the Criminal Law* (2010).

3 Criminal Law Act 1977, s 1. We discuss this further at paragraph 12.44 below.

4 The substantive offence of riot is found under section 1 of the Public Order Act 1986.

2A of the Suicide Act 1961, but has the same characteristics as an inchoate offence, namely that what is criminalised under these sections is preparatory conduct to achieve a particular result.[5]

12.6 There are a number of policy grounds justifying the criminalisation of such behaviour, including the desirability of early intervention in planned criminal activity, affording the police the opportunity to intervene in good time so as to prevent harm, and the deterrent effect inchoate criminal liability has on potential offenders.[6]

12.7 Our primary focus in the context of this Report is the use of the online environment to "encourage" crime; for example, the use of social media to encourage rioting or looting.

12.8 We also consider the extent to which other forms of inchoate liability, such as conspiracy and attempt, might apply to the key offences (communications offences, threats, harassment and privacy offences) that we have considered throughout this Scoping Report. At present, this is more of a theoretical possibility, as we are not aware of significant numbers of prosecutions of abusive and offensive online communications that are based on conspiracy or attempt.

12.9 We conclude by providing a number of examples to illustrate circumstances where inchoate liability might arise.

12.10 While the online environment is undoubtedly used to facilitate a variety of other forms ofinchoate crime, such as conspiracies to commit offences of violence and fraud, we do not consider this in any detail in this Chapter, as our focus is specifically on communication crimes, rather than all forms of criminal planning online.

12.11 We also do not consider the encouragement of terrorism offences and crimes associated with the sexual exploitation of children. Both make notable use of substantive inchoate offences, but are outside the scope of this Scoping Report.

OFFENCES OF ENCOURAGING AND ASSISTING CRIME

12.12 These offences are characterised by one party doing acts capable of encouraging or assisting another party to commit a specified criminal act. We consider the following provisions in the context of this Report:[7]

(1) sections 44 to 46 of the Serious Crime Act 2007, which form the overarching statutory framework of offences of encouraging the commission of an offence; and

(2) other substantive encouragement offences that arise in the context of this Report;

(a) section 19 of the Misuse of Drugs Act 1971 (inciting drug offences);

---

5 See A Ashworth and L Zedner, *Preventive Justice* (2014) pp 96 to 98.

6 Conspiracy and Attempts (2008) Law Commission Consultation Paper No 183, para 14.8.

7 This list does not include encouragement offences involving national security (Official Secrets Act 1920, s 7) or the administration of justice (Perjury Act 1911, s 7).

(b) sections 2 and 2A of the Suicide Act 1961 (encouraging suicide); and

(c) section 4 of the Offences against the Person Act 1861 (soliciting murder).

12.13 The substantive offences of stirring up hatred under the Public Order Act 1986 are discussed separately in Chapter 9.

Sections 44 to 46 of the Serious Crime Act 2007

12.14 The common law offence of inciting the commission of another offence was abolished by section 59 of the Serious Crime Act 2007 ("SCA 2007"). In its place, three offences were created:

- intentionally encouraging or assisting an offence;[8]
- encouraging or assisting an offence believing it will be committed;[9] and
- encouraging or assisting offences believing one or more will be committed.[10]

12.15 The offences under Part 2 of the SCA 2007 are particularly broad and overlap with other forms of inchoate liability.[11] Attention has been drawn in particular to the fact that:

(1) the most marginal conduct may suffice to amount to assistance or encouragement;

(2) in some cases the offences permit forms of double inchoate liability, whereby, for example, a person may be liable under section 44 for acts capable of assisting or encouraging another person to commit an inchoate offence under sections 45 or 46; and

(3) there need not be a completed principal/substantive offence and, in the case of sections 45 and 46, the fault element is less than an intention that the conduct element of the principal/substantive offence will be committed.[12]

12.16 According to Ministry of Justice statistics, since 2009 there have been 427 convictions where the offence of encouraging or assisting the commission of an offence was the principal offence charged.[13]

---

8 Serious Crime Act 2007, s 44.

9 Serious Crime Act 2007, s 45.

10 Serious Crime Act 2007, s 46.

11 D Ormerod and R Fortson, "Serious Crime Act 2007: The Pt 2 Offences" [2009] 6 *Criminal Law Review* 389, p 390.

12 See the Serious Crime Act 2007, s 47(2).

13 Ministry of Justice, *Criminal Justice System statistics quarterly: December 2017* (17 May 2018), available at https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2017.

12.17 Two relevant convictions that we discuss further below were those of Blackshaw and Sutcliffe, who pleaded guilty to using online platforms to encourage the crimes of riot, burglary and criminal damage during the 2011 London riots.[14]

Intentionally encouraging or assisting an offence

12.18 Section 44 of the SCA 2007 states:

> (1) A person commits an offence if–
>
> (a) he does an act capable of encouraging or assisting the commission of an offence; and
>
> (b) he intends to encourage or assist its commission.
>
> (2) But he is not to be taken to have intended to encourage or assist the commission of an offence merely because such encouragement or assistance was a foreseeable consequence of his act.

12.19 For example, where a person, D, posts on a blog encouraging another, P, to tweet threatening and racist messages to another, V, they may be liable for encouraging the commission of an offence under section 1 of the Malicious Communications Act 1988 ("MCA 1988"), or section 127 of the Communications Act 2003 ("CA 2003"), provided D intended to encourage such conduct. These substantive offences are discussed further in Chapter 4.

Encouraging or assisting an offence believing it will be committed

12.20 Section 45 of the SCA 2007 states:

> (1) A person commits an offence if–
>
> (a) he does an act capable of encouraging or assisting the commission of an offence; and
>
> (b) he believes–
>
> (i) that the offence will be committed; and
>
> (ii) that his act will encourage or assist its commission.

12.21 For example, this offence could be committed where D sends a message to another, P, encouraging P to burgle a victim's home so long as D believed that P was going to burgle the home, and would be encouraged to do so by the defendant's message.

Encouraging or assisting offences believing one or more will be committed

12.22 Section 46 of the SCA 2007 states:

> (1) A person commits an offence if–

[14] *R v Blackshaw* [2011] EWCA Crim 2312; [2012] 1 WLR 1126.

(a) he does an act capable of encouraging or assisting the commission of one or more of a number of offences; and

(b) he believes–

(i) that one or more of those offences will be committed (but has no belief as to which); and

(ii) that his act will encourage or assist the commission of one or more of them.

12.23 As we note at paragraph 12.67, a defendant pleaded guilty to the section 46 offence in relation to the encouragement of riot, burglary and criminal damage, after setting up a Facebook page encouraging rioting and looting in the context of the 2011 London riots.

Territorial application

12.24 The core elements of these three offences are given extended definitions by the remaining provisions under part 2 of the SCA. Of particular note are section 52 and schedule 4, which together set out the extra-territorial ambit of the offences. Three distinct instances are provided for:

(1) *Cases where the defendant's conduct takes place outside England and Wales but the victim is within England and Wales* – a person may commit an offence under sections 44 to 46 irrespective of where he or she is located, provided he or she knows or believes that what he or she anticipates might take place if the offence encouraged or assisted is committed will be wholly or partly in England or Wales.[15] Therefore, jurisdiction is determined by reference to the defendant's state of mind about where the anticipated act might take place rather than the location of the defendant at the time of the act.[16]

(2) *Cases where the defendant's conduct takes place within England and Wales but the victim is outside England and Wales* – a person may commit an offence under sections 44 to 46 where the victim is located outside England and Wales, provided any relevant behaviour of the defendant takes place wholly or partly in England or Wales and the anticipated offence is either (1) triable under the law of England and Wales if it were committed there (for example, murder);[17] or (2) amounts to an offence under the law in force in the place that the defendant is located (for example, theft).[18]

(3) *Cases where the defendant's conduct takes place outside England and Wales and the victim is outside England and Wales* – a person may commit an offence under sections 44 to 46 where both the initial act and the anticipated effect take place outside England and Wales provided that the defendant could be tried

15 Serious Crime Act 2007, s 52(1).

16 R Fortson, *Blackstone's Guide to the Serious Crime Act 2007* (2008) p 108.

17 Serious Crime Act 2007, sch 4, para 1.

18 Serious Crime Act 2007, sch 4, para 2.

under the law of England and Wales if he or she committed the anticipated offence in that place.[19]

Defence of acting reasonably

12.25 It is a defence to liability under sections 44 to 46 if the defendant can establish that they knew or reasonably believed "certain circumstances" to exist, and it was reasonable for the defendant to act as they did in those circumstances.[20] The Act does not prescribe what circumstances; this will depend on the facts of the case.

12.26 For example, in an online context, an animal activist might seek to argue that it was reasonable to write a blog post encouraging others to break into and record footage at abattoirs known to be using cruel and illegal methods to slaughter animals. If this argument was accepted, the activist would not be criminally liable under sections 44 to 46 of the SCA 2007.

Other substantive encouragement offences

12.27 In addition to the overarching offences in the SCA 2007, there exist specific substantive encouragement offences that may have applicability in the online environment. We outline three of these below.

Section 19 of the Misuse of Drugs Act 1971

12.28 It is an offence under section 19 of the Misuse of Drugs Act 1971 for a person to incite another to commit an offence under any other provision of the Misuse of Drugs Act 1971.[21] For example, it would be an offence under section 19 to incite the production of a controlled drug in the United Kingdom, as the production of a controlled drug is an offence under section 4(2)(a) of the Misuse of Drugs Act 1971.

12.29 Incitement is not necessarily synonymous with encouragement. The Divisional Court *in R v Marlow*[22] stated that to amount to incitement, encouragement must "involve words or actions amounting to a positive step or steps aimed at inciting another to commit a crime". This was accepted by the Court of Appeal in *R v Jones.*[23]

12.30 Given the breadth of offences under the SCA 2007, bringing a prosecution under those offences would be likely to be preferred.

---

19 Serious Crime Act 2007, sch 4, para 3.

20 Serious Crime Act 2007, s 50.

21 It is also possible to encourage the commission of the section 19 offence pursuant to section 44 of the Serious Crime Act 2007, but not sections 45 or 46. See Serious Crime Act 2007, s 49(4) and sch 3, pt 1, cl 9.

22 *R v Marlow* [1997] EWCA Crim 1833; [1998] 1 Cr App R (S) 273, cited in *R v Jones* [2010] EWCA Crim 925; [2010] 2 Cr App R 10 at [17].

23 [2010] EWCA Crim 925; [2010] 2 Cr App R 10.

12.31 Since 2008 there have been only 16 convictions where the offence under section 19 of the Misuse of Drugs Act 1971 was the principal offence charged.[24]

Encouraging or assisting suicide

12.32 It is an offence to do an act, or arrange for another person to do an act, that is capable of encouraging or assisting the suicide or attempted suicide of another person under sections 2 and 2A of the Suicide Act 1961. The maximum penalty is 14 years' imprisonment.

12.33 The offences were amended by section 59 of the Coroners and Justice Act 2009, in order to state the existing law more clearly and bring the terminology in line with part 2 of the SCA 2007. Section 44 of the SCA 2007 explicitly does not apply to complicity in the suicide of another.[25]

12.34 Importantly, the prosecution must demonstrate that the defendant "intended to encourage or assist suicide or an attempt at suicide".[26] The Director of Public Prosecutions ("DPP") advised the Parliamentary Committee considering the Bill that this would rule out circumstances such as a young person uploading morbid poetry or lyrics, as they would lack the necessary intention required for the offence.[27]

12.35 Crown Prosecution Service ("CPS") policy for prosecutors in respect of cases of encouraging or assisting suicide has been issued by the DPP.[28] The policy was issued in 2010 as a result of the decision of the Appellate Committee of the House of Lords in *R (Purdy) v DPP*,[29] which required the DPP "to clarify what his position is as to the factors that he regards as relevant for and against prosecution" in cases of encouraging and assisting suicide.[30] It was most recently revised in October 2014.

12.36 Since 2007, there have been 13 convictions where offences under sections 2 and 2A of the Suicide Act 2007 were the principal offences charged.[31]

Conspiring or soliciting to commit murder.

12.37 Section 4 of the Offences against the Person Act 1861 states:

---

24 Ministry of Justice, *Criminal Justice System statistics quarterly: December 2017* (17 May 2018), available at https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2017.

25 Serious Crime Act 2007, s 51A.

26 Suicide Act 1961, s 2(1)(b).

27 *Hansard* (HC), Public Bill Committee Debates, 5 February 2009, col 106, question 252 (Keir Starmer, Director of Public Prosecutions).

28 Crown Prosecution Service, *Suicide: Policy for Prosecutors in Respect of Cases of Encouraging or Assisting Suicide* (2014), available at https://www.cps.gov.uk/legal-guidance/suicide-policy-prosecutors-respect-cases-encouraging-or-assisting-suicide.

29 [2009] UKHL 45; [2010] 1 AC 345.

30 *R (Purdy) v Director of Public Prosecutions* [2009] UKHL 45; [2010] 1 AC 345 at [55].

31 Ministry of Justice, *Criminal Justice System statistics quarterly: December 2017* (17 May 2018), available at https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2017.

> Whosoever shall solicit, encourage, persuade, or endeavour to persuade, or shall propose to any person, to murder any other person, whether he be a subject of Her Majesty or not, and whether he be within the Queen's dominions or not, shall be guilty of a misdemeanour, and being convicted thereof shall be liable to imprisonment for life.

12.38 The scope of this offence was considered briefly in our recent scoping consultation paper and report on offences against the person.[32] We consider the elements of the offence below.

(1) *The victim* – the offence does not require the victim to be an identified person in being.[33] The offence includes incitement to kill people in generic categories, such as "Hindus, Jews and non-believers".[34]

(2) *The solicited person* – as with the victim, the solicited person need not be an identified person.[35] A general appeal to the public to murder someone would suffice. Although the solicitation must reach the solicited person,[36] their mind does not have to change.[37]

(3) *The solicitation* – the solicitation must be to kill, not merely to do serious harm.[38] This includes a solicitation to act as an accessory to murder.[39] In deciding whether the words amount to a solicitation, the jury will take account of the words used and the wider context in which they were made.[40]

(4) *The fault element* – the offence contains no explicit fault element. It has been suggested that the fault element is that the defendant must intend or believe that the other person, if he or she acts as incited, shall or will do so with the fault required for the offence.[41]

(5) *Jurisdiction* – the offence makes the solicitation of murder an offence in England and Wales, without proof that the inciter is British, that the proposed killer is British, or that the killing will be in England and Wales or that the proposed victim is British.[42]

---

32 Reform of Offences against the Person: A Scoping Consultation Paper (2014), Law Commission Consultation Paper No 217, paras 2.171 to 2.188, and 5.154 to 5.174; see also Reform of Offences against the Person (2015) Law Com No 361.

33 *R v Shephard* [1919] 2 KB 125.

34 *R v El-Faisal* [2004] EWCA Crim 456.

35 *R v Sheppard* [2010] EWCA Crim 65; [2010] 1 WLR 2779.

36 *R v Krause* (1902) 66 JP 121.

37 *R v Diamond* (1920) 84 JP 211.

38 *R v Bainbridge* (1991) 93 Cr App R 32.

39 *R v Winter* [2007] EWCA Crim 3493; [2008] *Criminal Law Review* 821.

40 *R v Diamond* (1920) 84 JP 211.

41 See D Ormerod and K Laird, *Smith, Hogan and Ormerod's Criminal Law* (15th ed, 2018) p 617.

42 *R v Abu Hamza* [2006] EWCA Crim 2918; [2007] QB 659.

12.39 An example where such a charge was not pursued was the case of Rhodri Phillips, who in 2016 wrote the following on Facebook in respect of business owner and anti-Brexit campaigner Gina Miller:

> £5,000 for the first person to "accidentally" run over this bloody troublesome first generation immigrant.

12.40 The decision not to prosecute was probably influenced by the difficulty in proving that the solicitation was for someone to "kill" Gina Miller, and to kill her with intent. Notwithstanding the unpleasant nature of the content, proof of these elements seems unlikely.

12.41 Ultimately, Phillips was successfully prosecuted for sending a menacing communication contrary to section 127(1) of the CA 2003.

CONSPIRACY

12.42 A criminal conspiracy involves an agreement between two or more persons to commit a crime.[43]

12.43 The Criminal Law Act 1977 replaced the broad common law offence of conspiracy with a statutory offence, preserving only common law conspiracy to defraud, conspiracy to do acts tending to corrupt public morals and conspiracy to outrage public decency.[44] Below we consider statutory conspiracy under the Criminal Law Act 1977 and the common law offences of conspiracy to do acts tending to corrupt public morals and outrage public decency.[45]

General statutory offence of conspiracy under section 1 of the Criminal Law Act 1977

12.44 There are six elements to the offence of statutory conspiracy under section 1 of the Criminal Law Act 1977:[46]

(1) an agreement;

(2) that a course of conduct will be pursued;

(3) the course of conduct will necessarily amount to the commission of an offence if carried out in accordance with the defendants' intentions;

(4) the defendants had an intention to agree;

(5) the defendants had an intention that the agreement will be carried out;

---

43 Criminal Law Act 1977, s 1.

44 The Law Commission has proposed abolishing the remaining common law conspiracy offences: Fraud (2002) Law Com No 276.

45 We do not consider the offence of conspiracy to defraud, as crimes against financial interests and property are outside the scope of this Report.

46 See D Ormerod and K Laird, *Smith, Hogan and Ormerod's Criminal Law* (15th ed, 2018) p 437.

(6) the defendants had an intention or knowledge as to any circumstances forming part of the substantive offence.[47]

12.45 The underlying policy of the statutory offence of conspiracy contained in the Criminal Law Act 1977 is reflected in the preceding 1976 Law Commission report:

> The crime of conspiracy should be limited to agreements to commit criminal offences: an agreement should not be criminal where that which it was agreed to be done would not amount to a criminal offence if committed by one person.[48]

12.46 Proceedings for conspiracy to commit summary offences can only be instituted with the consent of the DPP, or in some cases, the Attorney General.[49] This is important as a number of the key offences we consider in this report, such as "improper use of public electronic communications network" under section 127 of the CA 2003, relevant offences under the Data Protection 2018,[50] and the offences of "harassment"[51] and "stalking",[52] are summary offences.

12.47 Whilst the agreement must be complete such that a decision has been reached between the parties,[53] the courts have failed to define with precision what conduct suffices to constitute the completed agreement.[54] The offence lies in agreeing with another that a crime will be committed:

> What has to be ascertained is always the same matter: is it true to say ... that the acts of the accused were done in pursuance of a criminal purpose held in common between them?[55]

12.48 A person can be convicted of conspiracy even though he or she will not be involved in the commission of the substantive crime.[56]

12.49 Section 1(1)(b) of the Criminal Law Act 1977 also provides that, in a case of statutory conspiracy, the fact that the course of conduct relied on rendered the substantive offence impossible does not prevent a conviction for conspiracy. For example, if agreement is reached between two people to disclose private sexual photographs of

---

47 Criminal Law Act 1977, s 1(2). See *Saik* [2006] UKHL 18; [2007] 1 AC 18.

48 Conspiracy and Criminal Law Reform (1976) Law Com No 76, para 1.113.

49 See Criminal Law Act 1977, s 4(1) and (2).

50 Data Protection Act 2018, ss 170 and 171.

51 Protection from Harassment Act 1997, s 2.

52 Protection from Harassment Act 1997, s 2A.

53 *R v Walker* [1962] *Criminal Law Review* 458. See also G Williams, *Criminal Law: the General Part* (1953) p 212.

54 See D Ormerod and K Laird, *Smith, Hogan and Ormerod's Criminal Law* (15th ed, 2018) p 438.

55 *R v Meyrick* (1929) 21 Cr App R 94, p 102.

56 *R v Anderson* [1986] AC 27.

another[57] on Facebook, but the content is blocked by the platform before it is uploaded, the offence may still be committed.

12.50 A person is not guilty of a statutory conspiracy if the person or persons with whom he or she agrees are (a) his or her spouse, or civil partner; [58] (b) a person under the age of criminal responsibility; or (c) an intended victim of that offence or of each of those offences.[59]

Conspiracies to commit offences outside England and Wales

12.51 Section 1A of the Criminal Law Act 1977 governs agreements to commit offences outside England and Wales. This is summarised in *Smith, Hogan and Ormerod* in the following terms:

> The section applies where the pursuit of the agreed course of conduct would involve an act by one or more of the parties, or the happening of some event, in a place outside England and Wales which (a) would be an offence by the law of that place, and (b) would be an offence triable here but for the fact that it was committed abroad. Then, if, in England or Wales (a) a person became a party to the agreement, or (b) a party to the agreement did anything in relation to it before its formation, or did or omitted anything in pursuance of it, the agreement is indictable as a conspiracy, contrary to section 1(1) of the 1977 Act.[60]

12.52 Although agreements to commit offences outside England and Wales are provided for by the 1977 Act, it makes no express provision for either (1) agreements made abroad to commit an offence in England and Wales or (2) agreements made abroad to commit an offence abroad. Scenario (1), an agreement abroad to commit an offence in England and Wales, is caught by the common law.[61] Scenario (2) is not caught by the common law in England and Wales. This position is different to the SCA 2007, which makes provisions for both jurisdictional scenarios, as discussed at paragraph 12.24 above.

Common law offence of conspiracy to do acts tending to corrupt public morals or outrage public decency

12.53 As we noted in our 2015 report, Simplification of Criminal Law: Public Nuisance and Outraging Public Decency,[62] the common law offences of conspiracy to do acts tending to corrupt public morals or outrage public decency[63] remain available to prosecutors as they were specifically preserved by section 5 of the Criminal Law Act 1977.

---

57 Contrary to section 33 of the Criminal Justice and Courts Act 2015.

58 Civil Partnership Act 2007, sch 27.

59 Criminal Law Act 1977, s 2(2).

60 See D Ormerod and K Laird, *Smith, Hogan and Ormerod's Criminal Law* (15th ed, 2018) p 460.

61 *Somchai Liangsiriprasert v United States Government* (1990) 92 Cr App R 77; *R v Sansom* [1991] 2 QB 130; and *Re Goatley* [2002] EWHC 1209 (Admin).

62 Simplification of Criminal Law: Public Nuisance and Outraging Public Decency (2015) Law Com No 358, para 2.67.

63 See *Shaw v DPP* [1962] AC 220; *Knuller (Publishing, Printing and Promotions) Ltd v DPP* [1973] AC 435.

12.54 However, given the meaning of "outraging public decency" (discussed in Chapter 6) is identical in both the substantive offence and the conspiracy, it should still be pursued under section 1 of the Criminal Law Act 1977 (and for this reason we recommended that the common law conspiracy offence should be abolished).[64]

ATTEMPTS

12.55 The common law offences of attempt and procuring materials for crime[65] were repealed by the Criminal Attempts Act 1981 ("CAA 1981").[66] In their place, a statutory offence was created by section 1(1) of the Act.

12.56 Section 1(1) provides that a person may be guilty of attempting to commit an offence if:

> with intent to commit an offence to which this section applies, a person does an act which is more than merely preparatory to the commission of the offence …

12.57 Liability therefore turns on the defendant doing acts which are more than merely preparatory to the full offence with intent to commit a substantive offence.[67]

12.58 Only indictable offences may be pursued as an attempt, and the offences of conspiracy, aiding and abetting, encouraging or assisting suicide, and assisting an offender or concealing an offence are further excluded.[68] As we noted in relation to conspiracy, the exclusion of summary offences removes a large number of the core offences we have considered in this Report from consideration.

12.59 The offence under section 1 of the CAA 1981 is committed where the defendant does an act which is more than merely preparatory to the commission of an offence. "Merely" preparatory acts are therefore excluded from the ambit of the offence. Section 4(3) of the CAA 1981 first requires the judge to determine, as a question of law, whether the defendant's conduct is capable of being more than merely preparatory. It is then for the jury to determine for itself, as a fact, whether the conduct is or is not more than merely preparatory.

12.60 The fault element for attempts, although seemingly simple ("an intent to commit an offence"), is slightly more complex, and depends on the conduct, consequence and circumstance requirements of the substantive offence.[69]

12.61 Liability arises even through so called "impossible attempts":

---

64 Simplification of Criminal Law: Public Nuisance and Outraging Public Decency (2015) Law Com No 358, para 2.67.

65 See *R v Singh* [1966] 2 QB 53.

66 Criminal Attempts Act 1981, s 6.

67 See Conspiracy and Attempts (2008) Law Commission Consultation Paper No 183.

68 Criminal Attempts Act 1981, s 1(4).

69 For further discussion, see D Ormerod and D Perry (eds), *Blackstone's Criminal Practice 2019*, paras A5.79 to A5.81.

A person may be guilty of attempting to commit an offence to which this section applies even though the facts are such that the commission of the offence is impossible.[70]

12.62 In practice, the likelihood of an attempt prosecution for online abusive and offensive communications is low. Most of the relevant offences are summary, and therefore fall outside the scope of the CAA 1981. Further, while it is theoretically possible that an attempted indictable offence such as a threat to kill[71] could be committed online – for example if the threat was blocked by the server before reaching its target – it is unlikely that such conduct would come to the attention of law enforcement officials.

INCHOATE OFFENCES IN THE CONTEXT OF ABUSIVE AND OFFENSIVE ONLINE COMMUNICATIONS

12.63 While the online environment may be used to coordinate a wide range of criminal conduct, the application of inchoate liability in the context of "abusive and offensive" online communications is relatively limited.

Encouragement of crime online

12.64 The most relevant offences are the encouragement and assisting offences under the SCA 2007. There have been suggestions, for example, that these provisions may be used to prosecute audio or video content that encourages offences involving the use of knives, drugs or forms of group violence.[72] However, a general glorification of certain conduct, without an intention for a specific crime to be committed, would be difficult to fit within the terms of sections 44 to 46 of the SCA 2007. This contrasts with the specific offence of encouragement of terrorism under section 1 of the Terrorism Act 2006, which includes criminalising a statement which "glorifies the commission or preparation (whether in the past, in the future or generally) of such acts or offences".[73]

12.65 CPS prosecution guidance also suggests that the SCA 2007 may be used in cases where a person seeks to encourage others to commit communications offences, including "by way of a coordinated attack on a person".[74] Participants in our stakeholders' experiences event described how popular web forums were sometimes used to coordinate such attacks. Such conduct could potentially form the basis for inchoate liability for an offence under section 1 of the MCA 1988 or section 127 of the CA 2003, although we are not aware of such cases being prosecuted in practice.

12.66 Examples of use of encouragement offences in practice include prosecutions relating to comments posted on social media during the 2011 London riots that were specifically designed to encourage criminal conduct.

---

70 Criminal Attempts Act 1981, s 1(2).

71 Offences Against the Person Act 1861, s 16.

72 See: K Rawlinson, *Police may prosecute those who post videos glorifying violence* (30 May 2018), available at https://www.theguardian.com/uk-news/2018/may/30/police-prosecute-videos-glorifying-violence.

73 Terrorism Act 2006, s 1(3)(a).

74 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (21 August 2018), available at https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media.

12.67 In 2011, Jordan Blackshaw pleaded guilty to doing an act capable of encouraging the commission of riot, burglary and criminal damage contrary to section 46 of the SCA 2007, and was sentenced to four years' imprisonment.

12.68 He had used Facebook to set up and plan a public event called "Smash down in Northwich Town" with the purpose of encouraging criminal damage and rioting in the centre of Northwich. The website was aimed at his close associates, who he referred to as the "Mob Hill Massive", and his friends, but he also opened it to public view and included in the website references to ongoing rioting in London, Birmingham and Liverpool. He posted a message of encouragement on the website that read: "we'll need to get on this, kicking off all over".

12.69 Similarly, Perry Sutcliffe pleaded guilty to intentionally encouraging the commission of a riot contrary to section 44 of the SCA 2007 and was sentenced to four years' imprisonment.

12.70 He had used Facebook to construct a web page called "The Warrington Riots". On this webpage he included a photograph of police officers in riot equipment in a "stand-off position" with a group of rioters. He also included a photograph of himself and others in a pose described by police as "gangster-like". He sent invitations on Facebook to 400 of his contacts. In addition to his own Facebook contacts the website was also made available for general public viewing. Through the website, 47 people stated that they would go to the meeting.

12.71 The sentences of four years' imprisonment imposed on Blackshaw and Sutcliffe were upheld by the Court of Appeal.[75] Scaife writes that of particular significance in the judgment is the acceptance that whilst no actual harm flowed from the posts, citizens who read them were appalled and put in fear:

> The reference by the court to the offensive content of the post, suggests that there is an overlap with the CA 2003 and MCA 1988 as section 44 and 46 of the Serious Crime Act 2007 do not make reference to how the comments are received by a group of recipients or a specific intended recipient.[76]

12.72 Scaife also contrasts the above cases with the unreported case of *R v Bentley*. Bentley was charged with an offence under the SCA 2007 following the creation of a Facebook event page called "Wakey Riots". The case was thrown out after a one-hour trial as there was not enough evidence to disprove Miss Bentley's claim that the Facebook riot event was a joke, given that she posted messages such as "LMFAO".[77] However, while the defendants in *Blackshaw* and *Sutcliffe* had also claimed that the content they posted was a joke, unlike Bentley they ultimately pleaded guilty to the charges.

---

75 *R v Blackshaw* [2011] EWCA Crim 2312; [2012] 1 WLR 1126 at [75].

76 L Scaife, *Handbook of Social Media and the Law* (2015) p 173.

77 A commonly used acronym which signifies "laughing my fucking ass off".

Offence of encouraging suicide

12.73 So-called "suicide sites" have emerged as a serious problem online.[78] These websites are often highly graphic and include forums where suicide notes or suicidal intentions are posted.

12.74 As well as dedicated websites, online chat rooms may be used to discuss or encourage suicide. For example, in January 2003, a 21-year-old man in the United States streamed himself taking a lethal mix of drugs whilst 12 individuals in the chat room watched and encouraged his actions.[79]

12.75 Following amendments to the Suicide Act 1961 by the Coroners and Justice Act 2009, a person can commit an offence of encouraging or assisting suicide without any specific person being specified or identified. This covers instances where material is published online to unknown persons. As noted by Gillespie, one of the stated purposes of the Coroners and Justice Act 2009 amendments was to cater for suicide websites.[80]

12.76 The applicability of the amended sections to the online environment is also discussed in the CPS policy for prosecutors in respect of cases of encouraging or assisting suicide, which provides:

> In the context of websites which promote suicide, the suspect may commit the offence of encouraging or assisting suicide if he or she intends that one or more of his or her readers will commit or attempt to commit suicide…
>
> The amendments to section 2 of the Suicide Act 1961 are designed to bring the language of the section up-to-date and to make it clear that section 2 applies to an act undertaken via a website in exactly the same way as it does to any other act. [81]

12.77 Among the various factors identified by the CPS as suggesting prosecution is more likely to be in public interest factors tending in favour of prosecution include where:

> the suspect was unknown to the victim and encouraged or assisted the victim to commit or attempt to commit suicide by providing specific information via, for example, a website or publication.[82]

12.78 The Court of Appeal in *R v Howe*,[83] providing guidance as to relevant factors for a court to consider when sentencing "face to face encouragement or assistance", acknowledged

---

78 Y Jewkes, *Crime Online* (2007) p 2.

79 O Craig, "Chatmates watched internet suicide" (9 February 2003) available at https://www.telegraph.co.uk/news/worldnews/northamerica/usa/1421554/Chatmates-watched-internet-suicide.html.

80 A Gillespie, *Cybercrime: Key Issues and Debates* (2016) p 193.

81 Crown Prosecution Service, *Suicide: Policy for Prosecutors in Respect of Cases of Encouraging or Assisting Suicide* (2014), paras 20 to 25, available at https://www.cps.gov.uk/legal-guidance/suicide-policy-prosecutors-respect-cases-encouraging-or-assisting-suicide.

82 Crown Prosecution Service, *Suicide: Policy for Prosecutors in Respect of Cases of Encouraging or Assisting Suicide* (2014), para 43, available at https://www.cps.gov.uk/legal-guidance/suicide-policy-prosecutors-respect-cases-encouraging-or-assisting-suicide.

83 [2014] EWCA Crim 114; [2014] 2 Cr App R (S) 38 at [23].

that different considerations arise in cases of "remote encouragement" which would need to be addressed on another occasion.

Conspiracies and attempts

12.79 While crimes of conspiracy and attempt crimes have particular application in certain online contexts such as attempting to groom children, they are less obviously applicable to the main substantive offences we have considered in this Report. The two main reasons for this are:

(1) the majority of the offences relevant to offensive and abuse online communications are summary offences, and therefore excluded from attempt; and

(2) it is less likely that conduct amounting to conspiracies and attempts will come to the attention of law enforcement than conduct amounting to actual harm.

12.80 However, it is conceivable that some of the more serious offences could be prosecuted as conspiracy or attempt, for example:

(1) In a nasty family dispute, a conspiracy could be agreed between siblings to put another sibling in fear of violence through a series of email threats. This could be pursued as a conspiracy to commit an offence contrary to section 4 of the Protection from Harassment Act 1997.

(2) An attempt could be made by an angry ex-partner to disclose private sexual videos of their ex on YouTube in order to distress the ex. If YouTube were able to intercept the videos and prevent publication, but report the attempt to the authorities, a charge of an attempt to commit an offence contrary to section 33 of the Criminal Justice and Courts Act 2015 might be prosecuted.

Prosecution of encouragement, conspiracy and attempt

12.81 Below we consider the following issues that may arise in the online context of encouragement crimes:

(1) failed conspiracies and attempts;

(2) encouragement of offences not aimed at a particular individual; and

(3) encouragement falling short of suicide.

Failed conspiracies and attempts

12.82 A single letter or number that is mistaken when, for example, a person is typing in a Twitter handle, can completely change the intended recipient. In the example below, we consider the legal position where the commission of a substantive offence is impossible.

Example 1: misdirected messages

Linda agrees with Seth that they will both tweet at a well-known celebrity, using threatening words with the intention to put the celebrity in fear of violence. Seth provides Linda with the celebrity's Twitter handle to make the conduct more threatening. Unbeknownst to Linda and Seth, they have been misspelling the celebrity's name on Twitter. In addition, the celebrity has stopped using Twitter. As a result, none of Linda and Seth's messages are viewed by the celebrity.

12.83 We consider this example in the context of section 4 of the Protection from Harassment Act 1997 ("PHA 1997"), which provides that a person is guilty of an office if he or she:

(1) causes another to fear, on at least two occasions, that violence will be used against him, and

(2) knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

12.84 In the above example, the result element of the substantive offence is not fulfilled: it is impossible for the consequence element (1) above to be met. However, an inchoate crime may still be committed if the substantive offence is impossible.[84]

12.85 Considering first statutory conspiracy under section 1 of the Criminal Law Act 1977,[85] Linda and Seth intend the words to put the celebrity in fear of violence. They have satisfied the six elements of conspiracy referred to at paragraph 12.44, and the fact that it would have been impossible for their conduct actually to cause the celebrity distress is not fatal to establishing liability for an offence of statutory conspiracy. What must be proved is that they agreed that a course of conduct would be pursued (tweeting threatening words) which would amount to commission of the offence under the PHA 1997 if carried out in accordance with their intentions.

12.86 Next, considering section 1(2) of the Criminal Attempts Act 1981, which provides:

> A person may be guilty of attempting to commit an offence to which this section applies even though the facts are such that the commission of the offence is impossible.[86]

12.87 Applying this to the facts of the example, the issue is whether the act (tweeting threatening words) has been more than merely preparatory to the commission of the offence if the facts had been as Linda and Seth believed them to be (the tweets were read by the celebrity). As they had completed carrying out the act of harassment, and there was nothing more they could do to complete commission of the offence under

---

84 Criminal Attempts Act 1981, s 1(2).

85 In the case of common law conspiracy, impossibility *is* a general defence for common law conspiracies provided that the impossibility does not arise from the inadequacy of the means used to commit the offence. See *DPP v Nock* [1978] AC 979; [1978] *Criminal Law Review* 483.

86 Criminal Attempts Act 1981, s 1(2).

section 4 of the PHA 1997, in this case the act was more than merely preparatory. Linda and Seth may therefore be convicted of attempt, notwithstanding that the substantive offence was impossible by virtue of the fact that the victim could not see the tweets.

Encouragement not aimed at a particular individual

12.88 One common issue in the online environment is that a person may offer a general form of encouragement, rather than encouraging an identifiable person. Equally, the intended victim of an online offence may not be an identifiable person. In some investigations, it may be impossible to determine the participants or victims in an alleged offence.

> **Example 2: encouragement of gang violence**
>
> Jamie produces a rap video promoting his gang, the Reds. In it, he encourages the use of violence against a rival gang, the Blues. Andy, a member of the Reds, stabs Peter, a member of the Blues gang.

12.89 In this example, Jamie has issued a general form of encouragement to use violence against a rival gang, the Blues. Neither Andy, the person encouraged, nor Peter, the actual victim, are identified.

12.90 For the purpose of the offences under part 2 of the SCA 2007, neither of these facts are fatal to a conviction: Jamie has done an act capable of encouraging the commission of an offence and he intends to encourage its commission.

Encouragement falling short of suicide

12.91 As noted at paragraph 12.32 above, there is a specific substantive inchoate offence of encouraging suicide.

12.92 However, an issue of concern in the online environment is the existence of material encouraging harmful conduct that falls short of suicide. For example, there are websites promoting self-harm through cutting and eating disorders, such as anorexia and bulimia.

> **Example 3: encouragement of self-harm**
>
> Linda accesses a website where people discuss mental health issues. Linda starts a new thread promoting self-harm.

12.93 As Gillespie writes, there is no specific offence of self-harming. As a result, publicising or glorifying self-harm is not ostensibly criminal either.[87]

12.94 However, there is an argument – which is untested as far as we are aware – that the offence of causing grievous bodily harm with intent, contrary to section 18 of the Offences Against the Person Act 1861, could be used in this context. As we noted in our

[87] A Gillespie, *Cybercrime: Key Issues and Debates* (2016) p 200.

2015 Reform of Offences Against the Person report, the wording of this offence – "whosoever shall unlawfully and maliciously by any means whatsoever wound or cause any grievous harm to any person…" – is so wide that it could potentially include self-harm,[88] and therefore encouraging such harm could be an offence under sections 44, 45 or 46 of the SCA 2007. For that offence to be committed, the person who was self-harming would have to cause herself serious harm and intend to do so. If that is an offence, then anyone assisting or encouraging such behaviour (online or otherwise) could be guilty of an offence under sections 44 to 46 of the SCA 2007.

12.95 There are also other types of criminal offences that could conceivably catch the conduct in question; the communications offences and the offence under the Obscene Publications Act 1959 ("OPA 1959"). Online communications promoting self-harm would need to pass the threshold of "obscene, indecent or grossly offensive" to be prosecuted under section 127 of the CA 2003.[89] If considered obscene, its publication may be considered material that "depraves and corrupts" under section 2 of the OPA 1959.[90] Prosecution under these provisions, however, would need to ensure compatibility with the Human Rights Act 1998.[91]

CONCLUSION

12.96 Encouragement and other inchoate offences have some applicability in the context of offensive and abuse online communications, but in practice the scope for using them seems to be limited.

12.97 Relying as they do on the terms of substantive offences, inchoate offences do not themselves create legal disparity between the online and offline environment. However, as the majority of relevant offensive and abuse online communications offences are summary only, the limitations on the prosecution of conspiracy and attempt in summary offending effectively rules out most of the relevant charges.

12.98 Most directly relevant are the encouragement of crime offences; the SCA 2007 regime and specific substantive inchoate offences of encouraging crime. As we have noted in this Chapter, law enforcement agencies have raised the encouragement and "glorification" of crime online as an issue of concern, and the applicability of the criminal law in this context is not particularly clear.

12.99 Issues that we consider worthy of further consideration in this context are:

(1) Whether the "glorification" of certain types of violent crime online could amount to a criminal offence under the current law,[92] and if not, is there a case to reform the law, particularly with regard to certain very serious crime types (such as rape,

---

88 See Reform of Offences against the Person (2015) Law Com No 351, p 19.

89 Note that Gillespie is not convinced that these provisions would apply; see A Gillespie, *Cybercrime: Key Issues and Debates* (2016) p 201.

90 *John Calder (Publications) Ltd v Powell* [1965] 1 QB 509.

91 A Gillespie, *Cybercrime: Key Issues and Debates* (2016) p 201.

92 Section 1(3) of the Terrorism Act 2006, s1(3) is an example of an offence criminalising the glorification of the commission or preparation of acts of terrorism "whether in the past, in the future or generally". However, we do not consider this legislation further in this Chapter as offences relating to terrorism are outside the scope of this Report.

murder and grievous bodily harm)? For example, is there a case for an offence such as the offence of encouragement of terrorism contrary to section 1 of the Terrorism Act 2006?

(2) The potential harm that could be caused through the encouragement of self-harm (that falls short of suicide) online, and whether the criminal law is the right mechanism to address this.

12.100 There is also potential for greater use to be made of the SCA 2007 in the context of coordinated group attacks on individuals. This is an online phenomenon we have highlighted in other Chapters where we discuss harassment and stalking.

Chapter 13: Conclusion

THE NATURE OF THE PROBLEM

13.1 We have seen in this Scoping Report that there is a very broad array of harmful conduct that can be engaged in online, and that abusive and offensive communication has emerged as a serious social problem in recent years. The scale of abusive and offensive communication, and the complexity of the online environment is such that it is almost impossible to quantify precisely the degree of harm that is occurring. But almost anyone who has ever engaged online – through social media, online communities, online dating, online gaming, or even through reading comments in prominent news sites – will have experienced or witnessed one of the forms of offensive or abusive behaviour outlined in this Scoping Report.

13.2 The negative impacts of abusive online communications can be profound indeed, as we explore further in Chapter 3. At the most extreme end of the spectrum, online abuse can drive individuals to self-harm and suicide. More commonly, it can cause or contribute to psychological conditions such as depression and anxiety, and lead people to withdraw from social, professional and public life. Certain forms of communication, such as hate speech, can also have a more broadly damaging impact on society, contributing to the marginalisation of communities, and entrenching fear and discrimination.

THE ROLE OF THE CRIMINAL LAW

13.3 While the challenge of addressing the scale and reach of abusive and offensive online communications may seem overwhelming, we consider that the law, and in this particular context the criminal law, has an important role to play in punishing and deterring the most serious conduct, and in shaping community attitudes as to its unacceptability.

13.4 One of the participants in our stakeholders' experiences event summarised the situation aptly when she stated:

> Online abuse is like domestic violence in the 1980s. People used to say it was just something that happened. Police didn't step in on disputes between a husband and wife. But every part of society changed when prosecutions started being brought.

13.5 As with domestic abuse, the criminal law is clearly only one of the tools through which society can address the social harm of online abuse. The Government has committed to considering the broader online context – including the role of online platforms in enforcing appropriate standards – in its forthcoming Internet Safety Strategy White Paper.

13.6 Below we summarise our conclusions as to the current state of the criminal law, and the extent to which it provides equivalent protection online to that which is afforded offline. We also outline a number of areas where we consider that the current law fails

to provide the level of protection that is warranted, and suggest areas for further review and potential reform.

OUR ANALYSIS OF THE CURRENT STATE OF THE CRIMINAL LAW

13.7 Throughout this Scoping Report we have detailed the range of criminal offences – some very specific, and some very broad, which have been developed or applied to deal with the key forms of abusive and offensive communications. While we have identified a number of gaps and inconsistencies in the applicable law, we have concluded that in most cases abusive online communications are, at least theoretically, criminalised to the same or even a greater degree than equivalent offline behaviour.

13.8 This is particularly so given the broad reach of the offences under section 1 of the Malicious Communications Act 1988 ("MCA 1988") and section 127 of the Communications Act 2003 ("CA 2003"), which we discuss in further detail in Chapter 4.

13.9 In practice, however, it appears that practical and cultural barriers mean that not all harmful online conduct is pursued in terms of criminal law enforcement to the same extent that it might be in an offline context.

13.10 Further, our analysis has revealed that many of the applicable offences are not constructed and targeted in a way that adequately reflects the nature of offending behaviour in the online environment, and the degree of harm that it causes in certain contexts.

13.11 Therefore, while we do not consider there to be major gaps in the current state of the criminal law concerning abusive and offensive online communications, there is considerable scope to improve the criminal law in this area. In particular, we consider that reform could help ensure that the most harmful conduct is punished appropriately, while maintaining and enhancing protection for freedom of expression. It is towards these goals that we focus our recommendations for future law reform.

Practical and cultural barriers to enforcement of the criminal law

13.12 Before considering the terms of the offences themselves, it is important to understand the practical barriers to enforcement of the criminal law in this context. We discuss these in detail in Chapter 2, but in summary they are:

- the sheer scale of abusive and offensive communications, and the limited resources that law enforcement agencies and prosecutors have available to pursue these;
- a persistent cultural tolerance of online abuse, which means that even when reported, it is not always treated as seriously as offline conduct;
- the difficult balance that must be struck between protecting individuals and the community generally from harm, and maintaining everyone's fundamental human rights to freedom of expression;
- technical barriers to the pursuit of online offenders, such as tracing and proving the identity of perpetrators, and the cost of doing so; and

- jurisdictional and enforcement barriers to prosecution: the online environment is highly globalised, and even when overseas-based offenders have committed an offence in England and Wales, pursuing them may prove practically impossible or prohibitively expensive.

13.13 These are largely implementation issues for government and law enforcement agencies to grapple with, but must be borne in mind in any assessment of the effectiveness of the criminal law.

Communications offences

13.14 The two main communication offences that we have considered in this Report – section 1 of the MCA 1988 and section 127 of the CA 2003 – are both very widely cast, with section 127 in particular potentially drawing in a huge range of conduct.

13.15 From a prosecution perspective, there are some clear advantages to the current offences. As conduct crimes, which do not require proof of any particular harm having been caused, they create fewer evidential barriers to prosecution. For example, the evidence of a victim is usually not necessary to demonstrate that the offence has been committed. The broad, flexible wording of the offences also allows their use across a wide range of conduct and means they can adapt to changing forms of communication, as social media develop, and evolving forms of harm.

13.16 However, our analysis has also raised concerns that in certain contexts the threshold for criminal liability prescribed by the terms of these offences may be set too low.

13.17 In particular, as we note in Chapter 11, the offence of sending a "false" communication or "persistently [making] use of an electronics communication network" for the "purpose of causing annoyance, inconvenience or needless anxiety to another" under section 127(2) of the CA 2003 is very wide in scope.

13.18 This in effect leaves a huge degree of discretion to police and prosecutors, who have the unenviable task of determining the appropriate degree of offending at which prosecution is warranted. Further, as we note in Chapter 5, concepts such as "gross offensiveness" that are relied on in both the CA 2003 and MCA 1988 are ambiguous and subjective, making the law less certain and leading to inconsistent outcomes.

13.19 Finally, in Chapter 4 we note that the CA 2003 and MCA 1988 offences sit together somewhat awkwardly, and overlap to a significant degree. This is probably not in itself a sufficient basis for reform, but is an issue that could be addressed in the context of a general review of these offences.

13.20 In this first phase of the work we are not investigating possible alternative approaches, but we do consider that there is scope to improve these offences so that they reflect the harms and wrongs that the law is seeking to address more effectively, and more clearly distinguish between conduct which is criminal, and that which is not.

13.21 The Commission sees the potential advantages of a reformed approach as twofold:

- legitimate speech that should not be criminalised would be more clearly excluded; and

- law enforcement would be more clearly guided as to genuinely criminal conduct, and could better focus its resources on this.

13.22 Our view is that reform would not result in a substantial change in the degree of criminalisation of online abuse, but rather more effective targeting and labelling of it.

Recommendation 1.

13.23 The communications offences in section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003 should be reformed to ensure that they are clear and understandable and provide certainty to online users and law enforcement agencies.

Obscene and indecent communications

13.24 As we note in Chapter 6, the law of indecency and obscenity has a long history, which predates the emergence of the online environment. However, there is little doubt that the proliferation and extremity of obscene and indecent content has been amplified online.

13.25 While many of the fundamental concerns in relation to the law in this area are not limited to the online environment, there are a number of issues that are particularly prevalent in the online context and which we consider to be worthy of further consideration.

13.26 We also note the array of overlapping offences that might apply to indecent or obscene communication, and uncertainty over the extent of their application online.

Recommendation 2.

13.27 As part of the reform of communications offences, the meaning of "obscene" and "indecent" should be reviewed, and further consideration should be given to the meaning of the terms "publish", "display", "possession" and "public place" under the applicable offences.

Harassment and group offending

13.28 The offences of harassment and stalking are not particularly clearly defined in in the Protection from Harassment Act 1997. While case law has assisted considerably in defining the boundaries of these offences, there are still significant issues with the understanding of these offences amongst law enforcement officials and the general public.

13.29 These concerns are not limited to the online context, and we consider a general review of stalking and harassment laws to be outside the scope of this project.

13.30 However, as we note in Chapter 8, a specific concern that arises largely in an online context is the sometimes devastating impact of "pile on" abuse online.

13.31 In some cases, this might be relatively spontaneous, such as where a public figure writes something with which other members of society disagree, and receives a flood of abuse in response.

13.32 In other cases, it may be more coordinated, with for example online forums utilised to mobilise a stream of abuse towards a particular individual.

13.33 It is not clear that existing laws cope well with either of these circumstances. While there is scope for existing harassment and stalking laws (discussed further in Chapter 8) to be utilised for coordinated group harassment, the drafting and mechanism is complex, and not widely understood or utilised in this context.

Recommendation 3.

13.34 In addition to a reform of the communications offences, there should be a review to consider whether coordinated harassment by groups of people online could be more effectively addressed by the criminal law.

Hate crime

13.35 As we noted in our 2014 Hate Crime Report, there are significant inconsistencies in the way hate crime laws apply to different groups and in different contexts. In that Report we recommended a fundamental review of hate crime laws, and we welcome the Government's recent announcement that the Law Commission will be asked to conduct such a review.

13.36 Without wishing to pre-empt the findings of that review, two specific concerns we have identified in the course of our analysis are:

- the disproportionate targeting of women online, including through explicitly misogynistic language and sentiment; and
- the low prosecution rates for specific offences of stirring up hatred, and the pursuit of hate speech under more generic labels such as "gross offensiveness", which raises the question as to whether the criminal law needs to more directly describe and punish hate speech as such.

Recommendation 4.

13.37 The Law Commission's reviews of hate crime and communications offences should include consideration of:

- the disproportionate targeting of women online, including through explicitly misogynistic language and sentiment; and
- the effectiveness of the existing offences in labelling and punishing hate speech.

Privacy abuses

13.38 The online environment – and particularly the advent of social media – has fundamentally altered community expectations around privacy. While many now choose to share various aspects of their personal lives publicly, the scope to abuse online tools to violate the privacy of others has become a serious problem. We consider the criminal issues that arise in this regard in Chapter 10.

13.39 Particularly acute is the harm caused through the sharing of private sexual images online without the consent of the subject of those images. Many victims experience this as a form of sexual abuse, as well as a serious violation of their privacy, and the consequences can be devastating.

13.40 While the criminal law has sought to address this through the offence of "disclosing private sexual photographs and films with intent to cause distress",[1] we consider that emerging technological developments – specifically "deep fake" pornography – have already rendered this offence incapable of dealing adequately with the full range of harms that are occurring.

13.41 In addition to intimate images, our analysis suggests that the current law may provide insufficient remedies for other privacy abuses such as "outing" and "doxing", particularly when the degree of potential harm to victims is considered.

13.42 Even very serious non-consensual sharing of personal data is currently only punishable by a fine under the Data Protection Act 2018. Revealing the name of a complainant of a sexual offence similarly carries a maximum penalty of a fine only.

13.43 It is not clear that the available offences reflect the gravity of the offending behaviour and the harm caused in the most serious cases.

Recommendation 5.

13.44 The criminal law's response to online privacy abuses should be reviewed, considering in particular:

- whether the harm facilitated by emerging technology such as "deepfake" pornography is adequately dealt with by the criminal law; and
- whether there are adequate remedies to deal with the most serious privacy breaches.

False communications

13.45 While the online environment has led to an enormous democratisation of knowledge and learning, it has also become notorious for the amount of false and misleading

[1] Criminal Justice and Courts Act 2015, s 33.

information that it contains. This is a cause for concern; and the harm caused by "fake news" has been outlined recently by a parliamentary committee report.[2]

13.46 For the most part, false communications that are not connected to improper financial gain (such as fraud) or misleading commercial activity are not criminalised. There are exceptions; for example, there are certain public safety, electoral and justice offences that criminalise deliberately false statements. Civil consequences such as defamation may also apply where harm to a reputation is involved. However, in general, the criminal law does have not have a significant role in policing the truth of communications, whether they are made online or offline. Indeed, the (rarely prosecuted) offence of criminal libel was repealed in 2010 precisely because it was perceived to be an unjustified intrusion of the criminal law into the realm of free expression.

13.47 However, as we note in Chapter 11, the "false" communication offences under section 1 of the MCA 1988 and section 127(2) of the CA 2003 are surprisingly broadly cast, and were it not for prosecution guidance, and human rights protections, they could conceivably be used to police a huge array of low level speech.

13.48 Conversely, we have also noted that, notwithstanding the broad terms of the communications offences, certain potentially very harmful false communications are currently not criminalised where there is no malicious ulterior intent. For example, dangerously false health or safety advice. Given the extent of reliance placed on online sources, we consider that criminal deterrence in the most serious cases is worthy of further consideration.

Recommendation 6.

13.49 As part of the reform of communications offences the threshold at which malicious and "false" communications are criminalised should be reviewed.

Encouragement of crime online

13.50 In the final Chapter of this Report we note the very broad reach of the "encouragement" offences under the Serious Crime Act 2007, and their potential applicability to the online environment.

13.51 We also note that there are two contexts where it is unclear that certain encouragement conduct is criminalised, when arguably it should be, specifically:

(1) the "glorification" of certain types of violent crime (for example, the glorification of acid attacks or knife crime); and

(2) the encouragement of self-harm online.

[2] Disinformation and 'fake news': Interim Report, Report of the Digital, Culture, Media and Sport Committee (2017-19) HC 363, available at https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

Recommendation 7.

13.52 The glorification of violent crime online and the encouragement of self-harm online are issues which should be considered in the context of the review of communications offences.

Appendix 1: List of stakeholders

This Appendix lists the government departments and agencies, individuals and organisations who met us, attended one of our stakeholder events or corresponded with us during the currency of this project, and whose views have helped inform this Scoping Report.

GOVERNMENT DEPARTMENTS AND AGENCIES

Attorney General's Office

Cabinet Office

Crown Prosecution Service

Department of Digital, Culture, Media and Sport

Government Equalities Office

Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services

Home Office

Mayor's Office for Policing and Crime

Ministry of Justice

INDIVIDUALS

Dianne Abbott MP

Yvette Cooper MP

Stella Creasy MP

Caroline Criado-Perez

Sir Brian Leveson PC

Gina Miller

Rt Hon David Jones MP

Rt Hon Maria Miller MP

Rt Hon Nicky Morgan MP

Jess Phillips MP (Chair of All Parliamentary Public Group on Domestic Violence)

Lucy Powell MP

Folami Prehaye (Founder of Victims of Internet Crime)

Liz Saville Roberts MP

Dr Sunny Singh

ORGANISATIONS

Organisations which work closely with, or advocate for, people who experience abusive and offensive online communications

Anti-Bullying Alliance

Antisemitism Policy Trust

Campaign Against Antisemitism Community Security Trust

Demos

Digital Trust

Ditch the Label

Everyday Sexism Project

Fawcett Society

Galop

Internet Watch Foundation

Kidscape

Iranian and Kurdish Women's Rights Association

National Association of School Masters Union of Women Teachers

ManKind Initiative

Parentzone

Protection Against Stalking

Refuge

Respect

Rights of Women

Revenge Porn Helpline

Southall Black Sisters

Stonewall

Suzy Lamplugh Trust

TellMAMA

Trans Media Watch

Waymarks

Women's Aid

Young Minds

Technology companies and social media providers

Facebook

Google

Internet Service Providers Association

Oath

Twitter

Snap Group Limited

Civil liberties groups

Article 19

Index on Censorship

Open Rights Group

Other

The Bar Council

The National Trust

ACADEMICS

Chara Bakalis (Oxford Brookes University)

Professor Eric Barendt (University College London)

Professor Jim Barnes (University of Bedfordshire)

Dr Paul Bernal (University of East Anglia)

Neil Brown (Decoded: Legal)

Dr Kate Cook (Manchester Metropolitan University)

Professor Helen Fenwick (Durham University)

Rudi Fortson QC (Visiting Professor, Queen Mary University of London)

Professor Alisdair Gillespie (Lancaster University)

Timandra Harkness (University of Winchester)

Professor Julia Hornle (Queen Mary University of London)

Antoinette Huber (Liverpool John Moores University)

Professor Joseph Jaconelli (University of Manchester)

Professor Clare McGlynn (Durham University)

Professor Gavin Phillipson (Durham University)

Professor Andy Phippen (Plymouth University)

Professor Rob Procter (University of Warwick and Alan Turing Institute)

Associate Professor Jacob Rowbottom (University of Oxford)

Laura Scaife

Dr Emma Short (University of Bedfordshire)

Jo Smith (University of Leicester)

Professor Ian Walden (Queen Mary University of London)

Professor David Wall (University of Leeds)

CCS1018845550

978-1-5286-0848-0