Law Commission
Reforming the law

# Harmful Online Communications: The Criminal Offences

## A Consultation paper

Consultation Paper 248


**Law Commission**

**Consultation Paper 248**

# Harmful Online Communications: The Criminal Offences

# A Consultation Paper

**11 September 2020**



This publication is available at https://www.lawcom.gov.uk/project/reform-of-the-communications-offences/

# The Law Commission – How we consult

**About the Law Commission**: The Law Commission was set up by section 1 of the Law Commissions Act 1965 for the purpose of promoting the reform of the law. The Law Commissioners are: The Rt Hon Lord Justice Green, Chair, Professor Sarah Green, Professor Nicholas Hopkins, Professor Penney Lewis, and Nicholas Paines QC. The Chief Executive is Phillip Golding.

**Topic of this consultation**: We are consulting on reform of the communications offences (Malicious Communications Act 1988 and Communications Act 2003) in light of developments in online communication. We are also consulting on specific behaviours such as cyberflashing, pile-on harassment, and the glorification of both self-harm and violent crime.

**Geographical scope**: This consultation applies to the law of England and Wales.

**Duration of the consultation**: We invite responses from 11 September 2020 to 18 December 2020.

Responses to the consultation may be sent:

By email to online-comms@lawcommission.gov.uk OR

By post to Online Communications Team, Law Commission, 1st Floor, Tower, 52 Queen Anne's Gate, London, SW1H 9AG.

If you send your comments by post, it would be helpful if, whenever possible, you could also send them by email.

**Availability of materials**: The consultation paper is available on our website at https://www.lawcom.gov.uk/project/reform-of-the-communications-offences/

We are committed to providing accessible publications. If you require this consultation paper to be made available in a different format please email online-comms@lawcommission.gov.uk or call 020 3334 0200.

**After the consultation**: We will analyse the responses to the consultation, which will inform our final recommendations for reform to Government, which we will publish in a report.

**Consultation Principles**: The Law Commission follows the Consultation Principles set out by the Cabinet Office, which provide guidance on type and scale of consultation, duration, timing, accessibility and transparency. The Principles are available on the Cabinet Office website at: https://www.gov.uk/government/publications/consultation-principles-guidance.

**Information provided to the Law Commission**: We aim to be transparent in our decision-making, and to explain the basis on which we have reached conclusions. We may publish or disclose information you provide in response to Law Commission papers, including personal

information. For example, we may publish an extract of your response in Law Commission publications, or publish the response itself. We may also share responses with Government. Additionally, we may be required to disclose the information, such as in accordance with the Freedom of Information Act 2000. We will process your personal data in accordance with the General Data Protection Regulation.

Consultation responses are most effective where we are able to report which consultees responded to us, and what they said. If you consider that it is necessary for all or some of the information that you provide to be treated as confidential and so neither published nor disclosed, please contact us before sending it. Please limit the confidential material to the minimum, clearly identify it and explain why you want it to be confidential. We cannot guarantee that confidentiality can be maintained in all circumstances and an automatic disclaimer generated by your IT system will not be regarded as binding on the Law Commission.

Alternatively, you may want your response to be anonymous. That means that we may refer to what you say in your response, but will not reveal that the information came from you. You might want your response to be anonymous because it contains sensitive information about you or your family, or because you are worried about other people knowing what you have said to us.

We list who responded to our consultations in our reports. If you provide a confidential response your name will appear in that list. If your response is anonymous we will not include your name in the list unless you have given us permission to do so.

Any queries about the contents of this Privacy Notice can be directed to: enquiries@lawcommission.gov.uk.

# Contents

# Chapter 1: Introduction

## THE PROBLEM

1.1 The development of communications technology has far outpaced law reform. When we published our report in 1985[1] leading to the enactment of the Malicious Communications Act 1988, only 12.6% of UK households owned a home computer – and the internet wouldn't be invented for another four years.[2] Even in 2003, when the Communications Act 2003 was passed, only 46% of UK households had internet access.[3] It was another year before Facebook was released (and, even then, available only to select universities and colleges). Twitter was released in 2006. The first iPhone was not released until 2007, four years after enactment of the Communications Act. Nearly two decades later, in every single second that passes, nearly three million emails are sent,[4] nearly ten thousand Tweets are posted,[5] and over three quarters of a million WhatsApp messages are sent,[6] amongst the other c.95 terabytes of internet traffic per second.[7]

1.2 This revolution has offered extraordinary new opportunities to communicate with one another and on an unprecedented scale. However, those opportunities also present increased scope for harm: the physical boundaries of a home now afford no haven to the bullied; the domestic-abuser can exert ever greater control over the life of the abused; many thousands of people can now abuse a single person at once and from anywhere in the world. The examples are many.

1.3 As we noted in our Scoping Report on Abusive and Offensive Online Communications in 2018, the current criminal offences are ill-suited to addressing these harms.[8] The broad nature of the some of the offences does allow for their use across a wide range of conduct, although often the threshold of criminality when applied to the online space is set too low. Other forms of harmful communications (such as, for example, cyber-flashing) are either left without criminal sanction or without sufficiently serious criminal sanction.

---

1 Law Commission, *Poison-Pen Letters* (Law Com No 147, 1985).

2 J Schmitt and J Wadsworth, 'Give PC's a Chance: Personal Computer Ownership and the Digital Divide in the United States and Great Britain' (2002) Centre for Economic Performance, London School of Economics, p17.

3 Office for National Statistics, *Internet Access – households and individuals, Great Britain: 2018* (2018) p3.

4 Internet Live Stats, https://www.internetlivestats.com/one-second/#traffic-band (accessed June 2020).

5 The Number of Tweets per Day in 2020, https://www.dsayce.com/social-media/tweets-day/ (accessed June 2020).

6 WhatsApp Revenue and Usage Statistics (2020), https://www.businessofapps.com/data/whatsapp-statistics/ (accessed June 2020).

7 Internet Live Stats, https://www.internetlivestats.com/one-second/#traffic-band (accessed June 2020).

8 Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018).

## Freedom of expression

1.4 The need for a tailored legal response to these new forms of communication is not solely a product of changing harms. So long as the criminal law remains overlapping and ambiguous, there is a real risk that the freedom of expression – enshrined in long-standing English common law and in the European Convention on Human Rights ("ECHR") – will be eroded as the current offences expand haphazardly to address these new behaviours.

1.5 Indeed, even as drafted, we are concerned that the current offences are sufficiently broad that they could, in certain circumstances, constitute a disproportionate interference in the right to freedom of expression under article 10 of the ECHR. The criminalisation of grossly offensive speech is predicated on the notion that being offended is a harm that, when sufficiently serious, warrants the protection of the criminal law. This is a notion that the law should be slow to adopt. Ours is a society of many opinions; inescapably, then, there are as many avenues for causing offence – even serious offence. That someone is caused to be offended is no indication of the moral standing of the behaviour causing that offence. It is therefore not clear that offence – without more – is of the nature or level of harm sufficient to invite the interference of the criminal law.

1.6 Indeed, the courts have long been reluctant to permit that offence, in and of itself (ie without further harm), is a matter for the law. It is worth recalling the judgment of Sedley LJ in *Redmond-Bate v DPP*:[9]

> Free speech includes not only the inoffensive but the irritating, the contentious, the eccentric, the heretical, the unwelcome and the provocative provided it does not tend to provoke violence. Freedom only to speak inoffensively is not worth having.

1.7 Any criminal law solution to the problem therefore needs to offer effective protection from the harmful behaviours that have developed in the online space, whilst also ensuring that people have the freedom to express themselves, to interrogate orthodoxy, and to share ideas.

## THIS PAPER – BACKGROUND

1.8 In this Consultation Paper, we propose reform of the existing communications offences. Our work on the criminal law forms part of the work on Online Harms by the Department for Digital, Culture, Media and Sport ("DCMS") and the Home Office, and has been funded by DCMS.

1.9 The *Online Harms White Paper* published by DCMS and the Home Office in 2019 focusses on the regulation of platforms (eg Twitter and Facebook), whereas – as we note in the terms of reference below – this Paper is concerned to address the criminal law provisions that apply to individuals and not the liability of platforms. The criminal law is an important but, ultimately, limited part of the solution to online harms, which will require not just criminal law and regulatory reform but also education and cultural change.

---

9 *Redmond-Bate v DPP* [1999] EWHC Admin 733 [20].

1.10 This Paper forms part of the second phase of the Scoping Report that we published in November 2018. The purpose of that Report was to assess the extent to which the current law achieved parity of treatment between online and offline offending. We noted that there was considerable scope for reform, and identified three distinct possible strands of work, comprising: (i) reform and consolidation of the criminal laws dealing with online communications; (ii) a review of the law of hate crime in England and Wales; and (iii) a review of the law concerning the non-consensual taking and sharing of intimate images. From that Scoping Report has therefore flowed the following separately-funded but related Law Commission projects:

(1) Reform of the Communications Offences (this project);

(2) Hate Crime; and

(3) Taking, Making, and Sharing Intimate Images without Consent.

1.11 It is worth noting that the Hate Crime project and this project deal with different (albeit occasionally overlapping) issues. A proportion of online abuse can be, and often is, described as "online hate". Indeed, a significant subset of online abuse is targeted at people on the basis of their race, religion, sexual orientation, transgender status, or disability. However, not all abusive online communications amount to online hate. Equally, hate crime can encompass a wide range of behaviour – including, for example, acts of physical violence against people because of their race or sexual orientation, or criminal damage to businesses or places of worship – as well as hate speech.

### The terms of reference

1.12 The following terms were agreed with DCMS.

(1) The overall purpose of this project is to recommend reform of the criminal law relating to abusive and offensive online communications, following a period of public consultation.

(2) The project will cover:

(a) Reform and potential rationalisation of the current communications offences as they relate to online communication, with the aim of achieving a coherent set of offences that ensure online users are adequately protected by the criminal law.

(b) Where necessary, consideration of the meaning of "obscene", "grossly offensive", and "indecent", as well as the definitions of "publish", "display", "possession", and "public place" and of how we can best achieve clarity and certainty of the law for people communicating online.

(c) Consideration of online communications which amount to the glorification of self-harm and of violent crime and how these might be addressed in the context of any reform of the communication offences.

(3) In addressing the topics above, the Commission will be mindful to ensure that any recommendations for reform do not create incoherence or gaps in the criminal law as it relates to abusive and offensive communication offline.

(4) The Law Commission will also conduct a review to consider whether coordinated harassment by groups of people online could be more effectively addressed by the criminal law. This work on group harassment will form an extension of the online communications project.

### Topics not in scope

1.13 The following areas are outside the scope of this project:

(1) terrorist offences committed online;

(2) child sexual exploitation; and

(3) platform liability.

1.14 Any recommendations will therefore not address these topics.

## THIS PAPER – PROPOSALS AND SCOPE

1.15 The most significant proposal we make in this paper, in that it addresses the majority of the matters within our terms of reference, is a proposed new offence to replace the offences in section 1 of the Malicious Communications Act 1988 and section 127(1) of the Communications Act 2003. (We also propose reform of section 127(2) of the Communications Act). Rather than creating exhaustive definitions of words such as "offensiveness" etc, which we consider to be poor proxies for wrongfulness sufficient to justify criminalisation, we propose an offence based on the likelihood of harm absent reasonable excuse.

1.16 It is our view that this proposed offence will address many of the existing gaps in the law, though there are some exceptions. Most notably, some forms of cyber-flashing[10] receive either no or, depending on the context, insufficient sanction in the criminal law. We therefore propose that cyber-flashing should be a specific criminal offence (insofar as it isn't already caught by the exposure offence under section 66 of the Sexual Offences Act 2003) and, further, that it should be classed as a sexual offence. This reflects the sexual nature of the offending and the fact that the harms suffered by victim-survivors are akin to those of sexual offences. It also allows for sentencing that reflects the sexual nature of the offending (such as Sexual Harm Prevention Orders).

1.17 Further, it is our view that the proposed offence better meets the requirements of article 8 (the right to respect for private and family life, home and correspondence) and article 10 (freedom of expression) of the ECHR. By addressing the likelihood of harm directly rather than through proxies for that harm, the proposed offence is clearer than the existing law (without being so rigidly defined as to lack flexibility or

[10] The precise legal definition of cyber-flashing is a matter for discussion in this Consultation Paper (as there is no legal definition), though for present purposes it suffices to say that it is an act of digital exposure whereby images of the sender's genitals are sent digitally – via, for example, text message, email or Bluetooth – to another person.

allow easy side-stepping of the law). By requiring proof that the defendant lacked a reasonable excuse – which would include, say, participation in a debate of public interest – the court is able to balance the likely harm of the communication with the defendant's important right to freedom of expression. For example, the mere fact of someone being seriously offended by a politically sensitive communication will not, without more, establish the guilt of the defendant.

### "Online": technological neutrality and the scope of our proposed reforms

1.18 It is important at this stage to address the intended scope of our new offence. Though we often refer to the online space, as that presents some of the greatest challenges for the current law, we are not intending to narrow the current scope of the Malicious Communications Act 1988. The offence therein covers letters, electronic communications, and articles of any description that are sent. This covers communications that take place online (as they are electronic), but is broad enough to be technologically neutral; we would be concerned if, for example, iMessages (which are sent over the internet) and SMS text messages (sent over mobile telephone networks) were to be subject to different criminal law provisions.

1.19 The better distinction is therefore between "digital" communications, with which this report is concerned, and "in-person" communications, which do not fall within our terms of reference.

1.20 As will become clear in this Paper, it follows from the above that our new offence applies to a broader range of communications that currently fall within the scope of section 127 of the Communications Act 2003. That offence only governs communications sent over a "public electronic communications network" and, as we discuss, we do not think this a justifiable restriction on the scope of the offence. For example, communications over a peer-to-peer network (such as Bluetooth) would not fall within the scope of the offence.

1.21 In any case, we have tried not to constrain the offence to particular forms of offending. One of the reasons for proposing an offence that is technologically neutral (or as much as possible within the terms of reference) is to mitigate the risk that the law becomes redundant or unhelpful in the face of technological change.

### Harm and the communications offences

1.22 The communications offences sit within a larger set of offences that are characterised by communication, broadly speaking. We have noted some of them above (some forms of hate crime and sharing intimate images without consent). However, many other offences fall within that set. Fraud, for example, is an act of *misrepresentation*. Assault (causing someone to apprehend the immediate application of unlawful force) can also be committed through communication. Threats to kill are an offence under section 16 of the Offences Against the Person Act 1861. If you con someone into ingesting poison, then you have committed an offence under section 22 or 23 of that Act. Section 4A of the Public Order Act 1986 criminalises the use of threatening, abusive or insulting words. There are a great many examples. The harms addressed by each vary: the harm may be based on the violation of privacy, on economic harm, or on physical harm etc.

1.23 The communications offences are concerned with the harm that directly attends to the person who views (or, in the case of our proposed offence, was likely to view) the communication, and so our proposed offence is based on likely psychological harm caused by viewing the communication. As we note in chapter 4, many further harms result from abusive communications, and these can include not just psychological harms but also sometimes economic harms (if the victim has to leave their job, for example) or physical harm (if, say, the victim is driven to self-harm). In limiting the definition of harm for the purposes of proving the offence, we do not in any way imply that these harms are somehow less serious. However, as we discuss in chapter 5, we consider that psychological harm is the common denominator.

## STRUCTURE OF THIS PAPER

1.24 In Chapter 2, we outline the law relating to article 8 (the right to respect for private and family life, home and correspondence) and article 10 (freedom of expression) of the ECHR. These are important rights, but they are qualified. Any interference in these rights by the State must be adequately prescribed by law and be proportionate.

1.25 In Chapter 3, we recall some of the concerns raised in the Scoping Report and consider the limitations of the current law, and the propensity for the current offences both to under- and over-criminalise. In doing so, we address not only the MCA 1988 and CA 2003, but many of the other offences that could apply online (such as the Obscene Publications Act 1959, the Public Order Act 1986, amongst numerous others).

1.26 In Chapter 4, we consider the many harms that attend to online abuse. This is, in a sense, the other side of the scale from the freedom of expression concerns. The evidence we have received of the range of harms suffered by people of all backgrounds and characteristics has been enormously helpful in forming our views. Equally, it has been a poignant reminder of the urgency of our task.

1.27 In Chapter 5, we propose the new offence to replace section 127(1) of the Communications Act 2003 and section 1 of the Malicious Communications Act 1988.

1.28 We conclude with Chapter 6, which addresses a number of specific offences and matters to be considered under our terms of reference. These include:

- reform of section 127(2) of the Communications Act 2003;
- pile-on/group harassment;
- cyber-flashing;
- glorification of self-harm; and
- glorification of violent crime.

## ACKNOWLEDGEMENTS

1.29 During the drafting of this Consultation Paper, many people have generously given their time and shared their expertise with us. During the coronavirus pandemic, many

of those people have been under exceptional pressure yet chose to assist nonetheless. We are extremely grateful.

1.30 We would particularly like to extend our thanks to: The Alan Turing Institute; Article 19; Dr Chara Bakalis; Center for Countering Digital Hate; Community Security Trust; Crown Prosecution Service; Ditch the Label; Epilepsy Society; Sophie Gallagher; Galop; Paul Giannasi; Professor Alisdair Gillespie; Google; Professor Julia Hörnle; Interfaith ; Index on Censorship; Dr Kelly Johnson; Liberty; Magistrates Association; Professor Clare McGlynn QC (Hon); Dr Carrie-Anne Myers; Oath; Open Rights Group; Oxford Internet Institute; Dr Holly Powell-Jones; Professor Chris Reed; Refuge; Report Harmful Content; Professor Jacob Rowbottom; Dr Laura Scaife; Dr Adrian Scott; Dr Emma Short; Laura Thompson; Hugh Tomlinson QC; Twitter; Professor Ian Walden.

## THE PROJECT TEAM

1.31 We are grateful to the following members of the Law Commission who worked on this Consultation Paper: Dr Nicholas Hoggard (lead lawyer); Tatiana Kazim (research assistant); David Allen (lawyer); David Connolly (team manager); and Holly Brennan (research assistant at the earlier stages of the project).

# Chapter 2: Communication, human rights, and the criminal law

2.1 Any offence that criminalises communication will almost certainly be an interference with freedom of expression.[11] However, neither the long-standing common law right to freedom of speech nor the right under Article 10 of the European Convention on Human Rights ("ECHR") is absolute. Both rights are qualified. Some interferences with those rights can be justified. Nonetheless, the right comes first; it is the interference that requires justification.

2.2 The same is true of the right to respect for private and family life, home and correspondence under Article 8 of the ECHR. Restrictions on private communications constitute potential interferences with this right, and require justification.[12] However, not only is this right (like the right to freedom of expression) qualified, it also manifests itself as a positive obligation on States to ensure – so far as proportionate – respect for private life. Whilst the negative obligation requires that the State abstain from arbitrary interference in private communication, the positive obligation may require the State to adopt measures to ensure respect for Article 8 rights even as between individuals. Put simply, the positive obligation will sometimes favour restriction of communication.

2.3 Further, we recognise that communications have the potential to harm others. Indeed, the harmful impact of some abusive forms of communication, especially in an online context, can be severe. In Chapter 4, we discuss in detail the behaviours and harms that constitute and result from abusive online communications. This consideration must go into the balance, along with the right to freedom of expression (protected by Article 10) and the right to respect for private and family life, home and correspondence (protected by Article 8).

2.4 In this first chapter we explain the key rights that determine when it may be lawful and appropriate to criminalise communications – and when it is not. We discuss, first, the right to freedom of expression, protected by Article 10. We preface our analysis of Article 10 with a discussion of two considerations. First, we consider the importance of freedom of expression but, second, we also acknowledge the harmful nature of some forms of expression. We then go on to discuss the right to respect for private and family life, home and correspondence, protected by Article 8.

---

11 In theory, it may be possible to create an offence that criminalises only unprotected forms of expression; for discussion of unprotected expression, see below at 1.23-1.28. In practice, though, it is unlikely that an offence would be limited in this way. This is because it is only in extreme cases that expression is unprotected. In practice, then, it would be difficult (and not necessarily desirable) to create an offence that targets only unprotected expression.

12 We note, however, that some seemingly "private" communications are not protected by Article 8. We discuss this below at 1.70-1.78.

## THE IMPORTANCE OF FREEDOM OF EXPRESSION

2.5 The term "expression" is, in our usage, broader than the term "speech". Expression includes, but is not limited to, speech. It also covers other, non-speech forms of communication such as the symbolic burning of a cross, graffiti-painted images, or "dick pics" sent via Apple's "AirDrop" function.

2.6 This is consistent with the broad definition of "expression" adopted by the European Court of Human Rights ("ECtHR"). For example, in the case of *Mariya Alekhina and Others v Russia,*[13] the ECtHR held that an attempt by the punk band "Pussy Riot" to perform their song, *Punk Prayer – Virgin Mary, Drive Putin Away*, from the altar of Moscow's Christ the Saviour Cathedral was a form of expression covered by Article 10 of the ECHR: "that action, described by the applicants as a "performance", constitutes a mix of conduct and verbal expression and amounts to a form of artistic and political expression covered by Article 10."[14] In reaching this conclusion, the Court enumerated other examples of "expression" covered by Article 10, including the public display of dirty clothing near Parliament[15] and the pouring of paint on statues of Ataturk.[16] It follows that freedom of expression encompasses, but is not limited to, freedom of speech.

2.7 In his recent judgment in the case of *Miller v College of Policing,*[17] Mr Justice Julian Knowles, sitting in the High Court, emphasised the importance of freedom of expression. The judgment opens with a quote from the unpublished introduction to *Animal Farm* (1945) by George Orwell:

> If liberty means anything at all, it means the right to tell people what they do not want to hear.[18]

2.8 The judgment goes on to quote the well-known words of Sedley LJ in *Redmond-Bate v DPP*:[19]

> Free speech includes not only the inoffensive but the irritating, the contentious, the eccentric, the heretical, the unwelcome and the provocative… Freedom only to speak inoffensively is not worth having.[20]

2.9 The right to freedom of expression is protected under Article 10 of the ECHR. Below, we discuss in detail the protection afforded to freedom of expression by Article 10, and

---

13 *Mariya Alekhina and Others v Russia* (2019) 68 EHRR 14 (App No 38004/12).

14 *Mariya Alekhina and Others v Russia* (2019) 68 EHRR 14 (App No 38004/12) at [206].

15 *Tatár and Fáber v Hungary* App No 26005/08 and 26160/08.

16 *Murat Vural v Turkey* App No 9540/07, cited in *Mariya Alekhina and Others v Russia* (2019) 68 EHRR 14 (App No 38004/12) at [204].

17 *R (Miller) v College of Policing* [2020] EWHC 225, [2020] HRLR 10.

18 *R (Miller) v College of Policing* [2020] EWHC 225, [2020] HRLR 10at [1].

19 *Redmond-Bate v DPP* [1999] Crim LR 998 at [20].

20 *R (Miller) v College of Policing* [2020] EWHC 225, [2020] HRLR 10at [3], quoting *Redmond-Bate v DPP* [1999] Crim LR 998 at [20].

the limits it places on the lawful restriction of that freedom. However, it should be noted that, even before the ECHR was incorporated into UK law by the Human Rights Act 1998, freedom of expression had long been recognised by the common law. For example, in *Attorney General v Observer Ltd*, Lord Goff said, "we may pride ourselves on the fact that freedom of speech has existed in this country perhaps as long as, if not longer than, it has existed in any other country in the world."[21]

2.10 In *Free Speech: A Philosophical Enquiry,*[22] Frederick Schauer identifies three values commonly thought to be protected by rights to freedom of expression. These are:

(1) truth;

(2) democracy; and

(3) individual autonomy or self-fulfilment.

2.11 Citing the Canadian case of *R v Keegstra,*[23] L W Sumner says that these values "are now routinely rehearsed by courts in their adjudication of free speech issues."[24] Sumner's observation also holds true for the UK. Indeed, in *ex parte Simms*,[25] the House of Lords explained the instrumental importance of freedom of expression by reference to the same three values identified by Schauer:

> Freedom of expression is, of course, intrinsically important: it is valued for its own sake. But it is well recognised that it is also instrumentally important. It serves a number of broad objectives. First, it promotes the self fulfilment of individuals in society. Secondly, in the famous words of Mr. Justice Holmes (echoing John Stuart Mill), "the best test of truth is the power of the thought to get itself accepted in the competition of the market."…Thirdly, freedom of speech is the lifeblood of democracy. The free flow of information and ideas informs political debate. It is a safety valve: people are more ready to accept decisions that go against them if they can in principle seek to influence them. It acts as a brake on the abuse of power by public officials. It facilitates the exposure of errors in the governance and administration of justice of the country.[26]

2.12 Similarly, the ECtHR has emphasised in a number of cases that the right to freedom of expression is an "essential foundation of a democratic society" and a "basic condition for its progress and for the development of every man".[27]

---

21 *Attorney General v Observer Ltd* [1990] 1 AC 109 at 283.

22 F Schauer, *Free Speech: A Philosophical Enquiry* (1982).

23 *R v Keegstra* [1990] 3 SCR 697.

24 L W Sumner, "Criminalizing Expression: Hate Speech and Obscenity" in J Deigh and D Dolinko, *The Oxford Handbook of Philosophy of Criminal Law* (2011) p 18.

25 *R v Secretary of State for the Home Department, ex parte Simms* [2000] 2 AC 115.

26 *R v Secretary of State for the Home Department, ex parte Simms* [2000] 2 AC 115 at 126.

27 *Handyside v United Kingdom* (1976) 1 EHRR 737 (App No 5493/72) at [49].

2.13 Given the importance of freedom of expression, the burden of justification for criminalising expressive behaviour is weighty.

## HARMFUL FORMS OF EXPRESSION

2.14 An interference with freedom of expression will be easier to justify if the prohibited expression is harmful or has the potential to cause harm. It may once have been thought that speech cannot be harmful (consider the old adage "sticks and stones may break my bones but words can never hurt me"). However, there is now a body of theoretical literature arguing that speech (a subset of expression) is not, or at least not always, simply inert words or ideas. Instead, speech is often better understood as a kind of act: a "speech act".

2.15 Speech acts can, according to academics such as Professor Rae Langton, be harmful in various ways. Langton, drawing on J L Austin's seminal work *How to Do Things with Words*,[28] has argued that hate speech is a kind of speech act. Langton characterises hate speech as a harmful speech act of a particular kind: speech that does something distinctively harmful to a particular group.[29] According to Langton, speech acts may be harmful in a *constitutive* sense and a *causal* sense. [30] In other words, a speech act can be harmful in and of itself (the constitutive sense)[31] or harmful in terms of its effects (the causal sense).

2.16 The causal harms of speech acts include the emotional and psychological impact on the target, such as distress, anxiety, trauma, and so on. They also include negative impact on social attitudes, such as stirring up hatred or reinforcing widely-held negative stereotypes – whether actual or likely.

2.17 Drawing on Sumner's work, the causal harms of expressive behaviour can be further subdivided: causal harms may be *direct* or *indirect*. Harm is direct if "it results from exposure to the messages by members of the target group themselves."[32] Direct

---

28 J L Austin, *How to Do Things with Words* (1962).

29 R Langton, "The Authority of Hate Speech" (2018) 3 Oxford Studies in Philosophy of Law.

30 See for example, R Langton, "Hate Speech and the Epistemology of Justice" (2016) 10 *Criminal Law and Philosophy* 865, 867

31 The constitutive harms of speech acts may include: degradation or subordination of the target of the speech; ranking of the target in comparison to others; or placing of the target in a hierarchy; or legitimation or promotion of violence against the target. For example, by calling someone "vermin", or claiming that they are a monkey, the speaker ranks the subject of their speech as subhuman. This ranking is a constitutive harm of the speech act. To take another example, by saying "you deserve to be raped", the speaker legitimates sexual violence against the subject of their speech. In addition to the significant causal harm this speech may cause if someone who hears it is motivated to rape the victim, the legitimisation of sexual violence is a constitutive harm which arises in addition to or independently from sexual violence itself. The distinction between causal and constitutive harms is also endorsed elsewhere. For example, Article 19 (a non-governmental organisation) in their Hate Speech Toolkit distinguish between expression which is "considered to be harmful in itself for being degrading or dehumanising" (constitutive harms) and expression which is "considered to have a potential or actual harmful consequence" (causal harms). See Article 19, *'Hate Speech' Explained, A Toolkit* (2015), https://www.article19.org/data/files/medialibrary/38231/'Hate-Speech'-Explained---A-Toolkit-%282015-Edition%29.pdf (last visited 4 September 2020) at 10.

32 L W Sumner, "Criminalizing Expression: Hate Speech and Obscenity" in J Deigh and D Dolinko, *The Oxford Handbook of Philosophy of Criminal Law* (2011) p 24.

harms therefore include emotional and psychological harms suffered by the target. Harm is indirect if it "work[s] through the mediation of attitudes and conduct on the part of an audience other than the target groups themselves."[33] Indirect harms therefore include incitement of violence and more diffuse societal harms, such as diminished social cohesion, or reduced representation of certain social groups in positions of power.

2.18 In short, expression can be harmful in a variety of ways. Expression can involve:

(1) constitutive harms;

(2) direct causal harms; and

(3) indirect causal harms – which may be more or less diffuse.

2.19 We have learned from stakeholders that abusive online speech can be extremely harmful. In Chapter 4, we set out in detail the harms experienced by victims of, for example, pile-on harassment, cyber-flashing, hateful online speech, and other forms of online abuse. For the purposes of this chapter, we simply note our provisional view that the harms involved in online abuse may be a sufficiently compelling basis for interference with Article 10 rights – and Article 8 rights, discussed below from 1.60 – by way of suitably targeted, clear, and proportionate criminal offences.

## ARTICLE 10 ECHR

2.20 Article 10(1) of the ECHR provides:

> Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinematic enterprises.

2.21 The right to freedom of expression under Article 10 is qualified. Article 10(2) sets out the circumstances under which the right may be lawfully restricted. It provides:

> The exercise of these freedoms, since it carries with it duties and responsibilities, 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.

2.22 Hence, under Article 10(2), States are permitted to impose limited restrictions on freedom of expression to protect the interests specified in that paragraph. However, it is important to note that not all expression will engage Article 10 in the first place. As we explained in our Scoping Report and summarise in the next section, the ECtHR

---

[33] L W Sumner, "Criminalizing Expression: Hate Speech and Obscenity" in J Deigh and D Dolinko, *The Oxford Handbook of Philosophy of Criminal Law* (2011) p 24.

has drawn a line between protected and unprotected speech; the latter does not engage the right to freedom of expression under Article 10(1) at all.[34]

### Article 17 and unprotected speech

2.23 Whether or not speech is protected under Article 10(1) depends in part on Article 17, which prohibits the abuse of ECHR rights. Article 17 of the Convention provides:

> Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention.

2.24 Expressive activity falling within the scope of Article 17 is not protected by Article 10. In such cases, the ECtHR will not, therefore, engage in an analysis of whether a restriction on freedom of expression is justified under Article 10(2).

2.25 For example, in *Norwood v UK,*[35] Mr Norwood circulated a poster shortly after the 9/11 attacks which depicted the burning Twin Towers and carried the words “Islam out of Britain – Protect the British People”. Mr Norwood was convicted of an offence under the Public Order Act 1986 and applied to the ECtHR, claiming that his right to freedom of expression under Article 10 had been infringed. Mr Norwood’s case was found to be inadmissible on the grounds of Article 17:

> Such a general, vehement 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. The applicant's display of the poster in his window constituted an act within the meaning of Article 17, which did not, therefore, enjoy the protection of Articles 10 or 14 …[36]

2.26 By contrast, in *Soulas v France* – concerning the criminal conviction of the applicants for incitement of hatred and violence against Muslim communities, following the publication of a book entitled "The colonisation of Europe”, with the subtitle “Truthful remarks about immigration and Islam” – the Court found that Article 17 did not apply.[37] Given the nature of the terms used in the book, which the domestic courts found were intended to give rise in readers to a feeling of rejection and antagonism, the ECtHR held that there was no breach of the applicants’ Article 10 rights: the interference with freedom of expression was necessary in a democratic society. However, the ECtHR observed that the disputed passages in the book were not sufficiently serious to justify the application of Article 17.

---

34 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381 at paras 2.69 - 2.73.

35 *Norwood v United Kingdom* App No 23131/03 at [4].

36 *Norwood v United Kingdom* App No 23131/03 at [4].

37 *Soulas v France* App No 15948/03.

2.27 Some academics, like Professor Antoine Buyse, have criticised the ECtHR's application of the abuse of rights clause of Article 17 as being inconsistent.[38] (In addition, Buyse has argued that it is undesirable for cases to be declared inadmissible on the grounds of Article 17 at all: instead, cases involving freedom of expression should be assessed on the merits under Article 10, which allows for a balancing of the relevant interests.) However, ECtHR jurisprudence does, at least, indicate that the application of Article 17 is narrow: it only applies in extreme cases, where the expression in question aims to destroy the ECHR rights of another. This is a high bar. In *Norwood,* the Court said:

> The general purpose of Article 17 is to prevent individuals or groups with totalitarian aims from exploiting in their own interests the principles enunciated by the Convention.[39]

2.28 Our provisional view is, therefore, that the application of Article 17 to online abuse will be relatively rare. For example, while abusive, transphobic speech might deny a person's self-determined gender, it is unlikely that such speech would fall foul of Article 17. Denial of a person's gender may be deeply humiliating and distressing. It may interfere with an individual's Article 8 right to respect for private life, of which gender identity has been held by the ECtHR to be a part.[40] However, it probably does not amount to conduct aimed at the *destruction* of Convention rights. In most cases, Article 10 will be engaged by online abuse. We must, therefore, consider the extent to which the criminalisation of online abuse is compatible with Article 10.

### What does compliance with Article 10 require?

2.29 If Article 10 is engaged, the ECtHR must determine whether the restriction on freedom of expression is lawful under Article 10(2). The ECtHR's analysis proceeds in four stages. The ECtHR must determine:

(1) the existence of an interference;

(2) whether the interference was prescribed by law;

(3) whether the interference pursued a legitimate aim; and

(4) whether the interference was necessary in a democratic society.[41]

---

38 A Buyse, "Dangerous Expressions: The ECHR, Violence and Free Speech" (2014) 63(2) *International & Comparative Law Quarterly* 491.

39 *Norwood v United Kingdom* App No 23131/03.

40 See, for example, *Christine Goodwin v United Kingdom* (2002) 35 EHRR 18 (App No 28957/95). For further discussion of Article 8 rights, and the balancing of Article 8 and Article 10 rights, see below.

41 See, among other authorities, *Karácsony v Hungary* (2016) 64 EHRR 10 (App No 42461/13).

### Was there an interference?

2.30 The bar for finding the existence of an interference with the right to freedom of expression under Article 10(1) is low. In *Miller,*[42] Mr Justice Knowles described the approach of the ECtHR as follows:

> …the Strasbourg court's general approach to protecting freedom of expression under the Convention is to provide very wide protection for all expressive activities. The Court has done this in part by forging a very broad understanding of what constitutes an interference with freedom of expression. The approach of the Court has essentially been to find any State activity which has the effect, directly or indirectly, of limiting, impeding or burdening an expressive activity as an interference.[43]

2.31 This does not mean that any measure that may have some impact on freedom of expression will constitute an interference. To constitute an interference an action must amount to a so-called *Handyside* restriction: a formality, condition, restriction or penalty imposed in response to speech.[44] Hence, in *Miller,* Mr Justice Knowles found that "the mere recording by the police of the Claimant's tweets as non-crime hate speech pursuant to HCOG…[45] did not amount to an interference within the meaning of Article 10(1)." The judge recognised that "the mere act of recording speech may have a chilling effect on the speaker's right to freedom of expression." However, he nonetheless found that "the mere recording without more is too remote from any consequences [to] amount to a *Handyside* restriction."[46]

2.32 That being said, the ECtHR has found that restrictions falling short of a criminal prohibition amounted to an interference with Article 10(1). These include: a disciplinary sanction;[47] dismissal of an employee;[48] and an injunction.[49] Criminal limitations on freedom of expression, such as the existing communications offences – section 127 of the Communications Act 2003 ("CA 2003") and section 1 of the Malicious Communications Act 1988 ("MCA 1988") – clearly constitute an interference with Article 10(1). Indeed, in *DPP v Collins,* it was held that "section 127(1)(a) does of course interfere with a person's right to freedom of expression."[50]

2.33 That the communications offences constitute an interference with the right to freedom of expression is not, of course, enough to establish that they are incompatible with Article 10. This is only the first stage of the analysis. The substance of our criticism of

---

42 *R (Miller) v College of Policing* [2020] EWHC 225, [2020] HRLR 10.

43 *R (Miller) v College of Policing* [2020] EWHC 225, [2020] HRLR 10 at [175].

44 *Handyside v UK* (1976) 1 EHRR 737 (App No 5493/72) at [49].

45 "HCOG" is an acronym for the College of Policing's *Hate Crime Operational Guidance*.

46 *R (Miller) v College of Policing* [2020] EWHC 225, [2020] HRLR 10 at [176].

47 See, for example, *Engel and others v the Netherlands* (1979-80) 1 EHRR 647 (App No 5100/71, 5101/71, 5102/71, 5354/72, and 5370/72).

48 See, for example, *Vogt v Germany* (1996) 21 EHRR 205 (App No 17851/91).

49 See, for example, *The Sunday Times v United Kingdom* (1979) 2 EHRR 245 (App No 6538/74*)* at [49].

50 *DPP v Collins* [2006] UKHL 40, [2006] 1 WLR 2223 per Lord Bingham at [14].

the current law lies at the second stage of the analysis: whether the interference is prescribed by law.

### Was the interference prescribed by law?

2.34 Regarding the second stage of the analysis, in *Sunday Times v United Kingdom* it was held that, for a law to be compliant with this aspect of the Convention right, a citizen must be able to foresee, if necessary with "appropriate advice", the legal consequence a given action may entail.[51]

2.35 The Grand Chamber of the ECtHR has since made clear that Article 10 "not only requires that the impugned measure should have a legal basis in domestic law, but also refers to the quality of the law in question, which should be accessible to the person concerned and foreseeable as to its effects".[52] The court "must ascertain whether [the provision] is sufficiently clear to enable a person to regulate his/her conduct and to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail".[53]

2.36 Hence, an interference will be "prescribed by law" where:

(1) the interference in question has some basis in domestic law;

(2) the law is adequately accessible; and

(3) the law is formulated so that its application is sufficiently foreseeable.[54]

2.37 For our purposes – that is, considering the adequacy of the existing communications offences and possibilities for reform – the third of these factors is particularly relevant.

2.38 In our Scoping Report, we noted widespread criticism of the use of vague terms such as "grossly offensive" under the existing communications offences: section 127 of the CA2003 and section 1 of the MCA 1988. Such criticism was based on concerns about freedom of expression and came from academics, journalists, lawyers, and human rights organisations such as Big Brother Watch and the Open Rights Group. We must, therefore, consider the extent to which criminal provisions couched in vague terms like "grossly offensive" are consistent with freedom of expression as protected by Article 10, and particularly whether they are consistent with the requirement that any interference with Article 10 is "prescribed by law".

2.39 In the case of *Akçam v Turkey,* the ECtHR found that Article 301 of the Turkish Criminal Code, which made it an offence to "publicly degrade the Turkish nation",[55] amounted to a violation of the applicant's Article 10 rights on the following grounds:

---

51 *The Sunday Times v United Kingdom* (1979) 2 EHRR 245 (App No 6538/74) at [49].

52 *Karácsony v Hungary* (2016) 64 EHRR 10 (App No 42461/13) at [123].

53 *Akçam v Turkey* (2011) 62 EHRR 12 (App No 27520/07) at [91]; similarly, *Grigoriades v Greece* (1999) 27 EHRR 464 (App No 24348/94) at [37].

54 R Clayton and H Tomlinson, *The Law of Human Rights* (2nd edn 2010) 15.299.

55 Article 301, Turkish Criminal Code.

> In the Court's opinion… the scope of the terms under Article 301 of the Criminal Code… is too wide and vague and thus the provision constitutes a continuing threat to the exercise of the right to freedom of expression. In other words, the wording of the provision does not enable individuals to regulate their conduct or to foresee the consequences of their acts. As is clear from the number of investigations and prosecutions brought under this provision… any opinion or idea that is regarded as offensive, shocking or disturbing can easily be the subject of a criminal investigation by public prosecutors.[56]

2.40 Applying this reasoning to section 127 of the CA 2003 and section 1 of the MCA 1988, and to possible new offences making use of vague terms like "grossly offensive", it may seem that such provisions are in tension with Article 10. And yet, in the case of *DPP v Collins* – which, admittedly, was decided several years before *Akçam v Turkey* – the House of Lords held that the criminalisation under section 127 of communications which are "grossly offensive" was compatible with Article 10. In reaching this decision, Lord Bingham found that the restriction was "clearly prescribed by statute".[57]

2.41 It should also be noted that, in the case of *Singhal v Union of India*,[58] the Indian Supreme Court invalidated section 66A of the Information Technology Act of 2000 in its entirety, on the grounds that it used "completely open ended, undefined and vague language"[59] including the term "grossly offensive" (as well as the terms "annoyance" and "inconvenience", amongst others). The Supreme Court held "there is no demarcating line conveyed by any of these expressions – and that is what renders the Section unconstitutionally vague."[60]

2.42 However, in *Akçam v Turkey* the ECtHR was apparently persuaded, not (or, at least, not only) by the vague language of the provision itself, but by contextual factors: the high volume of prosecutions brought under Article 301 and the nature of the behaviour prosecuted. In the circumstances, it was clear that Article 301 could be easily used to prosecute "any opinion or idea that is regarded as offensive, shocking or disturbing". Attention was paid to the way the term had been interpreted in practice, not only to the term itself.

2.43 The judgment of the Grand Chamber of the ECtHR in *Karácsony v Hungary*[61] makes plain the fact-sensitive nature of the inquiry. In the judgment, it was observed that since "the law must be able to keep pace with changing circumstances… many laws are inevitably couched in terms which, to a greater or lesser extent, are vague".[62] But a provision couched in vague language may, even in the absence of previous application, be sufficiently precise if it is "interpreted and applied according to

---

56 *Akçam v Turkey* (2011) 62 EHRR 12 (App No 27520/07) at [93].

57 *DPP v Collins* [2006] UKHL 40, [2006] 1 WLR 2223 at [14], by Lord Bingham of Cornhill.

58 *Singhal v Union of India* (2015) Write Petition (Criminal) No 167 of 2012.

59 *Singhal v Union of India* (2015) Write Petition (Criminal) No 167 of 2012 at [74].

60 *Singhal v Union of India* (2015) Write Petition (Criminal) No 167 of 2012 at [76].

61 *Karácsony v Hungary* (2016) 64 EHRR 10 (App No 42461/13).

62 *Karácsony v Hungary* (2016) 64 EHRR 10 (App No 42461/13) at [124].

practice".[63] Hence, the Court found that the imposition of a disciplinary sanction, in the form of a fine, for conduct "gravely offensive to parliamentary order"[64] was compatible with Article 10: the vague term "gravely offensive" was rendered more precise by parliamentary practice. The Court was clearly persuaded by contextual factors:

> By reason of their specific status, members of parliament should normally be aware of the disciplinary rules which are aimed at ensuring the orderly functioning of Parliament… rules similar to those in Hungary exist in many European States and they are all couched in comparably vague terms…The Court considers that the applicants, on account of their professional status of parliamentarians, must have been able to foresee, to a reasonable degree, the consequences which their conduct could entail, even in the absence of previous application of the impugned provision.[65]

2.44 This suggests that the Article 10 compatibility of a criminal law provision couched in vague terms will depend, at least in part, on the practice according to which the provision is interpreted and whether this renders it sufficiently precise, such that the consequences of a defendant's conduct could have been reasonably foreseen. For example, the House of Lords in *R (Purdy) v DPP*[66] made clear that prosecutorial codes could, in theory, render a vague or ambiguous criminal law provision sufficiently precise to meet the requirements of Article 10.

2.45 In this regard, the CPS *Guidelines on prosecuting cases involving communications sent via social media*, published in 2013 and updated in 2016 and 2018, have improved the compatibility of the communications offences with Article 10. The publication of these guidelines was prompted by the conviction of Paul Chambers under the "menacing" limb of section 127(1) of the CA 2003, after he wrote a Tweet saying "Crap! Robin Hood Airport is closed! You've got a week and a bit to get your shit together otherwise I am blowing the airport sky high!!" Chambers was eventually acquitted two years after his initial conviction, but his case attracted the attention of prominent figures like Stephen Fry and brought section 127 into disrepute.[67]

2.46 In order to avoid such cases being brought, and prompted by the criticism of section 127 more generally, the CPS guidelines state that prosecutors should *only* proceed with cases under section 1 of the MCA 1988 or section 127 of the CA 2003 if the communication is *more than*:

(1) offensive, shocking or disturbing; or

(2) a satirical, iconoclastic or rude comment; or

---

63 *Karácsony v Hungary* (2016) 64 EHRR 10 (App No 42461/13) at [124].

64 *Karácsony v Hungary* (2016) 64 EHRR 10 (App No 42461/13) at [17].

65 *Karácsony v Hungary* (2016) 64 EHRR 10 (App No 42461/13) at [126].

66 [2009] UKHL 45, [2010] 1 AC 345.

67 See C Bakalis, "Rethinking cyberhate laws" (2018) 27(1) *Information & Communications Technology Law* 86, 101.

(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".[68]

2.47 The CPS guidelines also make clear the importance of context, including the characteristics of the intended recipient:

> 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?[69]

2.48 While this guidance does offer some clarification, we do not think it is satisfactory "to have in existence an offence that is", as Chara Bakalis puts it, "considered so broad that the CPS has to police itself".[70] One possibility for reform would be to provide a statutory definition of terms like "grossly offensive". Alternatively, a communications offence that does not rely on such vague terms would represent an improvement from an Article 10 perspective. We discuss these possibilities in more detail in Chapter 5.

### Did the interference pursue a legitimate aim?

2.49 An interference with Article 10(1) will only be justified if it pursues one of the legitimate aims set out in Article 10(2): national security, territorial integrity, public safety, and so on.

2.50 Clayton and Tomlinson state that, in practice, there are few disputes about whether an interference falls within the scope of one or more of the listed aims.[71] They do suggest, however, that the legitimate aim relied upon will be relevant to the breadth of the "margin of appreciation" the ECtHR affords the State.[72] The margin of appreciation determines how far the Court will leave the practical application of Article 10 in specific cases to the national institutions of the State in question. It seems clear that the Court will provide a greater margin of appreciation to the State where the interest being protected is national security rather than a matter of confidentiality.

---

68 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (last revised 21 August 2018), https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (last visited 4 September 2020).

69 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (last revised 21 August 2018), https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (last visited 4 September 2020).

70 C Bakalis, "Rethinking cyberhate laws" (2018) 27(1) *Information & Communications Technology Law* 86, 101.

71 R Clayton and H Tomlinson, *The Law of Human Rights* (2nd edn 2010) 15.305.

72 R Clayton and H Tomlinson, *The Law of Human Rights* (2nd edn 2010) 15.305.

2.51 It may be thought that the legitimate aim most obviously being pursued by the existing communications offences is the prevention of crime. However, when considering whether a criminal offence is itself compatible with Article 10, the aim of preventing crime cannot meaningfully be invoked, since the offence determines whether the proscribed behaviour is a crime in the first place. Instead, another aim must be relied upon. In our view, a communications offence may pursue the legitimate aims of public safety, protection of health or morals, or protection of the reputation or rights of others. As we explain in the Scoping Report and in Chapter 4, the types of harm that can arise from abusive online communications are manifold. They include:

(1) psychological 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.

2.52 In our view, criminal laws to protect people, and society, from such harms may constitute measures in pursuance of the legitimate aims of public safety, protection of health or morals, or protection of the reputation or rights of others.

### Was the interference necessary in a democratic society?

2.53 ECtHR jurisprudence makes clear that "necessary" is not synonymous with "indispensable" but nor is it synonymous with "desirable" or "useful".[73] Instead, as held by Lord Hope in *Shayler*, citing *Handyside*, "the word 'necessary' in article 10(2) introduces the principle of proportionality."[74]

2.54 Lord Sumption in *Bank Mellat* set out a four-stage "test" for determining the proportionality of an interference with a Convention right and held that:

> …the question depends on an exacting analysis of the factual case advanced in defence of the measure, in order to determine (i) whether its objective is sufficiently important to justify the limitation of a fundamental right; (ii) whether it is rationally connected to the objective; (iii) whether a less intrusive measure could have been used; and (iv) whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.[75]

2.55 In his dissenting judgment, Lord Reed, drawing on the Canadian case of *R v Oakes*[76] formulated the fourth stage slightly differently: "whether, balancing the severity of the measure's effects on the rights of the persons to whom it applies against the

---

[73] See, for example, *Handyside v United Kingdom* (1976) 1 EHRR 737 (App No 5493/72) at [48].

[74] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [57] (Lord Hope of Craighead).

[75] *Bank Mellat v Her Majesty's Treasury (No 2)* [2013] UKSC 39, [2014] AC 700 at [20] (Lord Sumption).

[76] *R v Oakes* [1986] 1 SCR 103.

importance of the objective, to the extent that the measure will contribute to its achievement, the former outweighs the latter".[77]

2.56 Such "tests" are directed towards answering the basic question of whether the means used were proportional to reach the aim, where the "aim" is one of those listed in Article 10(2) and the "means" is the measure that interferes with the right protected under Article 10(1). The "means" might, for example, be an order to pay damages for defamation, an injunction against publication, or a search of a newspaper's premises. The type of measure with which we are primarily concerned in this Consultation Paper is a criminal offence.

2.57 In order to find that an interference is "necessary in a democratic society" – that is, proportionate – and compatible with Article 10, the Court must be satisfied that there is a "pressing social need" for the interference. This is for a Member State to assess, in light of ECtHR jurisprudence:

> The Contracting States have a certain margin of appreciation in assessing whether such a need exists, but it goes hand in hand with a European supervision, embracing both the law and the decisions applying it, even those given by independent courts.[78]

2.58 As we state above, the "margin of appreciation" determines how far the ECtHR will leave the practical application of Article 10 in a given circumstance to a Member State to decide. When it comes to laws criminalising communications, the State is likely to have more latitude in relation to a communication that, say, threatens national security than it is in relation to, say, an abusive communication causing emotional or psychological harm to an individual.

2.59 Even accepting that the State has some margin of appreciation – albeit a lesser margin than if national security were the relevant aim – we doubt whether the existing communications offences could be considered "necessary in a democratic society". Discussing the offences under section 127 of the CA 2003 and section 1 of the MCA 1988 and, in particular, the criminalisation of communications that are "grossly offensive", "obscene", or "indecent", Chara Bakalis writes:

> It is difficult to see how proscribing such words would come within the Art 10(2) exceptions, as it is unlikely to be seen as 'necessary in a democratic society' to outlaw communications simply based on their gross offensiveness, indecency or obscenity. Trying to repress ideas or language simply because we do not like them is not sufficient within a liberal western democracy.[79]

---

77 *Bank Mellat v Her Majesty's Treasury (No 2)* [2013] UKSC 39, [2014] AC 700 at [74] (Lord Reed).

78 *Lingens v Austria* (1986) 8 EHRR 407 (App No 9815/82) at [39]. See also, for example, *Janowski v Poland* (2000) 29 EHRR 705 (App No 25716/94), *Tammer v Estonia* (2003) 37 EHRR 43 (App No 41205/98).

79 C Bakalis, "Rethinking cyberhate laws" (2018) 27(1) *Information & Communications Technology Law* 86.

## ARTICLE 8 ECHR

2.60 Any restriction on communications must also be consistent with Article 8 of the ECHR. Article 8(1) provides:

> Everyone has the right to respect for his private and family life, his home and his correspondence.

2.61 Like the right to freedom of expression under Article 10, the right to respect for private and family life, home and correspondence under Article 8 is qualified. Article 8(2) provides:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

2.62 In order to ensure consistency with Article 8, a restriction on communications could do one of the following: it could avoid catching communications protected by Article 8(1) of the ECHR (right to respect for private and family life, home and correspondence); or it could ensure that any limitations on communications protected by Article 8 are sufficiently clear, proportionate and necessary, in accordance with Article 8(2).

2.63 However, this alone will not be sufficient to ensure that the State meets its obligations under Article 8. As we say in the introductory remarks at the beginning of this chapter, Article 8 imposes positive as well as negative obligations on the State. This means that Article 8 functions not only as a limit on the lawful criminalisation of communications; the positive obligations it imposes on the State count in favour of the restriction of communications in some circumstances.

### When is Article 8 engaged?

2.64 Article 8 protects four interests:

(1) private life;

(2) home;

(3) family; and

(4) correspondence.

2.65 Article 8 is generally considered to be one of the most open-ended of the Convention rights; it protects a growing range of diverse interests, provided they fit under one of

the four aforementioned categories. A specific interest may fall within the scope of Article 8 even if it is not explicitly mentioned in the Article.[80]

2.66 The ECtHR has repeatedly stated that "private life" is "a broad term not susceptible to exhaustive definition".[81] For example, in *Aksu v Turkey*[82] – concerning a book entitled "The Gypsies of Turkey" which, the applicant complained, portrayed Gypsies as being engaged in illegal activities, as polygamists, and as aggressive, and which contained other humiliating and debasing remarks about Gypsies – the ECtHR adopted an expansive concept of "private life" which, it held, includes one's sense of identity as a member of a group:

> The notion of personal autonomy is an important principle underlying the interpretation of the guarantees provided for by art.8. It can therefore embrace multiple aspects of the person's physical and social identity. The Court further reiterates that it has accepted in the past that an individual's ethnic identity must be regarded as another such element. In particular, any negative stereotyping of a group, when it reaches a certain level, is capable of impacting on the group's sense of identity and the feelings of self-worth and self-confidence of members of the group. It is in this sense that it can be seen as affecting the private life of members of the group.[83]

2.67 *Aksu v Turkey*[84] concerned the State's positive obligations under Article 8. We discuss these positive obligations in more detail below, at 1.87-1.94. At this point we simply note that the range of interests protected by Article 8 is broader than may appear at first blush. As well as ethnic identity, the category "private life" has been held to encompass other aspects of "physical and moral integrity"[85] and personal development and autonomy,[86] including sexual orientation[87] and gender identity.[88] It also includes "privacy" rights, such as the right to one's image[89] and protection of reputation.[90] Under the category "home", Article 8 has been held to include an

---

80 European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights* (last updated 30 April 2020), https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (last visited 04 September 2020).

81 See, for example, *Bărbulescu v Romania* App No 61496/08 at [70], *Nicolae Virgiliu Tănase v Romania* App No 41720/13 at [126], and *Aksu v Turkey* (2013) 56 EHRR 4 (App No 4149/04) at [58].

82 *Aksu v Turkey* (2013) 56 EHRR 4 (App No 4149/04).

83 *Aksu v Turkey* (2013) 56 EHRR 4 (App No 4149/04) at [58].

84 *Aksu v Turkey* (2013) 56 EHRR 4 (App No 4149/04).

85 *X and Y v the Netherlands* (1986) 8 EHRR 235 (App No 8978/80) at [22].

86 See, for example, *Niemietz v Germany* (1993) 16 EHRR 97 (App No 13710/88) and *Pretty v United Kingdom* (2002) 35 EHRR 1 (App No 2346/02).

87 See, for example, *Burghartz v Switzerland* (1994) 18 EHRR 101 (App No 16213/90) and *Dudgeon v the United Kingdom* (1982) 4 EHRR 149 (App No 7525/76).

88 See, for example, *Christine Goodwin v United Kingdom* (2002) 35 EHRR 18 (App No 28957/95).

89 *Von Hannover v Germany (No 2)* (2012) 55 EHRR 15 (App No 40660/08).

90 *Axel Springer AG v Germany* (2012) 55 EHRR 6 (App No 39954/08).

individual's business premises,[91] and the Court does not rule out the possibility that it could include training centres and venues for sports events and competitions.[92] "Family" has likewise been interpreted expansively, to mean the real existence in practice of close personal ties.[93]

2.68 When considering the compatibility of communications offences with Article 8, the relevant interest will often fall under the fourth category: "correspondence". "Correspondence" has been held to cover – at least in principle – many forms of electronic and online communication including emails,[94] data stored on computer servers,[95] and even internet usage,[96] as well as communications using older technologies (telephone calls,[97] letters,[98] and so on).

2.69 However, these forms of communication will not automatically be covered by Article 8. In the context of communications sent from business premises, the Court has stated that a reasonable expectation of privacy is a significant though not necessarily conclusive factor in determining whether a communication falls within the scope of Article 8.[99]

2.70 Accordingly, "reasonable expectation of privacy" was a key factor in the recent decision in *B C and others v Chief Constable Police Service of Scotland,*[100] in which the question for the Court was whether the use of private WhatsApp messages as a basis for misconduct proceedings was a breach of the senders' Article 8 rights. In this case, Lord Bannatyne, sitting in the Outer House of Scotland's Court of Session, held that the petitioner police officers (whose WhatsApp group messages were passed on to the disciplinary unit of the force) had no reasonable expectation of privacy in respect of those messages.[101]

2.71 In reaching this decision, Lord Bannatyne's starting point, following Lord Toulson's judgment in *JR38*[102] and Laws LJ's judgment in *R (Wood) v Commissioners of Police*

---

91 *Niemietz v. Germany* (1993) 16 EHRR 97 (App No 13710/88).

92 *National Federation of Sportspersons' Associations and unions (FNASS) and Others v France* App No 48151/11).

93 See, for example, *Paradiso and Campanelli v Italy* (2017) 65 EHRR 2 (App No 25358/12).

94 See, for example, *Bărbulescu v Romania* App No 61496/08.

95 *Wieser and Bicos Beteiligungen GmbH v Austria* (2008) 46 EHRR 54 (App No 74336/01).

96 *Copland v United Kingdom* (2007) 45 EHRR 37 (App No 62617/00).

97 *Klass and Others v Germany* (1980) 2 EHRR 214 (App No 5029/71) and *Malone v the United Kingdom* (1985) 7 EHRR 14 (App No 8691/79).

98 *Niemietz v Germany* (1993) 16 EHRR 97 (App No 13710/88).

99 *Bărbulescu v Romania* App No 61496/08.

100 2019 SLT 875.

101 *B C and others v Chief Constable Police Service of Scotland and others* 2019 SLT 875 at [173].

102 [2015] UKSC 42, [2016] AC 1131.

*of the Metropolis*,[103] was that correspondence is within the scope of Article 8 protection:

> It is noteworthy for the purposes of this case that the scope of Article 8 covers the "zone of interaction" between the individual and others. I consider that it is clear that correspondence between individuals whether by means of paper or electronic communication can form part of the zone of interaction and therefore part of the core right protected by Article 8.[104]

2.72 The judgment goes on to make clear that there can, in general, be a reasonable expectation of privacy in relation to correspondence in the form of messages sent in a WhatsApp group. Lord Bannatyne noted that WhatsApp groups have the following features: members are notified when someone new joins the group; at this point, they can withdraw from the group if they wish; and, moreover, new members cannot see messages sent prior to their joining the group. These features were contrasted with the "entirely open and public"[105] character of communications on other social media platforms. In light of these features, it was held that "having regard only to the characteristics of 'WhatsApp' an ordinary member of the public using such could have a reasonable expectation of privacy".[106]

2.73 The decisive factor was, instead, the public role of police officers in society. In the judgment it is strongly implied that, in most other cases, WhatsApp users would have a reasonable expectation of privacy vis-à-vis their personal WhatsApp messages. The petitioner police officers had, however, subscribed to special standards of conduct in order to ensure that public confidence in the police was maintained, and these standards placed a limitation on their reasonable expectation of privacy that does not apply to ordinary people:

> The limitation can, I think, be described thus: if their behaviour in private can be said to be potentially in breach of the Standards in such a way as to raise doubts regarding the impartial performance of their duties then they have no reasonable expectation of privacy.[107]

Therefore, "the police officer in such a situation is in a different position from an ordinary member of the public".[108]

2.74 Given that the police officers had subscribed to these standards of conduct, they were "exchanging messages within a group of people whom they knew were under a positive obligation to report messages of the [relevant] type… where originating from

---

103 [2009] EWCA Civ 414, [2010] 1 WLR 123.

104 *B C and others v Chief Constable Police Service of Scotland and others* 2019 SLT 875 at [129].

105 2019 SLT 875 at [137].

106 2019 SLT 875 at [150].

107 2019 SLT 875 at [168].

108 2019 SLT 875 at [168].

other constables".[109] Therefore, they did not have a reasonable expectation of privacy in respect of such messages.

2.75 Notably, though, Lord Bannatyne was not persuaded by counsel for the respondents' references to various other examples of situations where messages sent in WhatsApp groups had been reported to university authorities or leaked to the press:

> I accept that it may happen that a person who joins a WhatsApp group makes public the content of what has been exchanged within the group. However, equally in the example I gave where confidences were exchanged in a house between friends one of those friends may breach the confidence. That does not undermine the individual's reasonable expectation of privacy. The exchanging of any information in a private context always carries with it the risk of breach of the confidence. Thus an individual's reasonable expectation may turn out to have been misplaced. However, it does not follow that the individual did not have a reasonable expectation of privacy.[110]

2.76 Hence, it was not the mere likelihood of messages being leaked or reported that undermined the police officers' reasonable expectation of privacy; it was the positive obligation on the part of the police officers to report one another for sending messages which violated the standards of conduct to which they had all subscribed.

2.77 Even so, the limits of this reasoning are unclear, and the decision raises the possibility that WhatsApp messages sent in a range of other circumstances may not be considered "private" for the purposes of Article 8. At the very least, the same reasoning could also be extended to other groups of professionals, such as lawyers and judges.

2.78 In short, some seemingly "private" communications may not engage Article 8 at all. However, there remains a significant proportion of online communications which are protected by Article 8. Criminalisation of such communications is lawful only as prescribed under Article 8(2).

### Negative obligations under Article 8

2.79 Article 8 is, like Article 10, a qualified right. To decide whether any restriction on Article 8 rights is lawful, the ECtHR's analysis will follow the same structure set out above at 1.29. The ECtHR must determine:

(1) the existence of an interference;

(2) whether the interference was prescribed by law;

(3) whether the interference pursued a legitimate aim; and

(4) whether the interference was necessary in a democratic society.

---

109 2019 SLT 875 at [172].

110 2019 SLT 875 at [142].

2.80 Hence, even in respect of private correspondence or other communications falling within the scope of Article 8, the State may adopt restrictive measures – up to and including criminal sanctions – provided that the interference is prescribed by law, pursues a legitimate aim, and is necessary in a democratic society.

2.81 Regarding the analysis under the first stage – the existence of an interference – the bar is, as in the case of Article 10, low. Much of the ECtHR jurisprudence is devoted either to the preliminary point – whether Article 8 is engaged at all – or to the latter stages of the analysis, under (2) to (4).

2.82 The analysis under stages (2) to (4) will be much the same as in relation to Article 10. Regarding the second stage – whether the interference was prescribed by law – any offence criminalising communications that fall within the scope of Article 8 must be sufficiently clear to enable a person to regulate their conduct and to reasonably foresee the legal consequences of a given action. Here again, vague terms like "grossly offensive" may present a problem.

2.83 Regarding the third stage, a criminal offence must pursue one of the legitimate aims set out at Article 8(2): these are likely to be public safety, the protection of health or morals, or for the protection of the rights and freedoms of others. Here again, criminal laws to protect people, and society, from the manifold harms arising from abusive online communication – including communications within the scope of Article 8 – may constitute measures in pursuance of the legitimate aims of public safety, protection of health or morals, or protection of the reputation or rights of others.

2.84 Regarding the fourth stage – whether the interference was necessary in a democratic society – the restriction (in this case, a criminal offence) must be proportionate to the legitimate aim pursued. We are unconvinced that this will be the case if the criminal offence is based, not on harmfulness, but on "indecency" or "gross offensiveness".

2.85 Indeed, "indecency" presents particularly acute problems in the case of private messages. For example, in the Scoping Report, we raised a concern that "indecent" for the purposes of the CA 2003 (given the lack of definition or guidance in case law) could cover private "sexting" between two consenting adults. We cited Alisdair Gillespie in support of this view:

> 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.[111]

2.86 In our provisional view, the criminalisation of private, sexual messages between consenting adults is – in the absence of any additional features, for example, that the messages concerned sexual activities with a child – not only "extraordinary" (as Gillespie puts it), but potentially incompatible with Article 8.

---

[111] A Gillespie, "Obscene conversations, the internet and the criminal law" [2014] *Criminal Law Review* 350, 359.

### Positive obligations under Article 8

2.87 In addition to the State's negative obligations not to interfere directly with Article 8 rights, except as prescribed under Article 8(2), the State is also under positive obligations to protect a person's Article 8 rights from interference by third parties.

2.88 The State's positive obligations in respect of Article 8 were acknowledged in *Aksu v Turkey*.[112] The task for the ECtHR was to determine whether the Turkish courts ought to have upheld the applicant's civil claim by awarding him non-pecuniary damages and banning the distribution of the book "The Gypsies of Turkey" (which, as we mentioned above, the applicant complained of due to its negative portrayal of Gypsies). The Court confirmed that Article 8 imposes positive obligations on the State to ensure respect for private life as between individuals:

> Furthermore, while the essential object of art.8 is to protect the individual against arbitrary interference by the public authorities, it does not merely compel the state to abstain from such interference: in addition to this negative undertaking there may be positive obligations inherent in the effective respect for private life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.[113]

2.89 The positive obligation encompasses a range of measures. For our purposes, it is important to note that these can include criminal offences, and effective enforcement thereof. For example, in *RB v Hungary* – a case concerning various instances of harassment, violence, and threats against people of Roma origin by right-wing paramilitary groups – the ECtHR confirmed that the positive obligation of a State to secure respect for private life can encompass conducting investigations into discriminatory events and the implementation of effective criminal law mechanisms.[114] This case, and other similar cases such as *Király and Dömötör v Hungary*,[115] specifically concern discriminatory conduct, including verbal threats, of a kind that may – if committed in the jurisdiction of England and Wales – amount to hate crime. They do not concern abusive communications more generally.

2.90 However, the judgment in *Király and Dömötör v Hungary*[116] seems to suggest that abusive communications which are not necessarily linked to discrimination against a particular group could nonetheless be deemed to interfere with the right to respect for private life. This would be the case if, for example, the communication affects "psychological integrity" by negatively affecting "feelings of self-worth and self-confidence" or consists of a threat resulting in a "well-founded fear of violence and humiliation" (even if this threat does not actually materialise).[117]

---

112 *Aksu v Turkey* (2013) 56 EHRR 4 (App No 4149/04).

113 *Aksu v Turkey* (2013) 56 EHRR 4 (App No 4149/04) at [59].

114 *RB v Hungary* (2017) 64 EHRR 25 (App No 64602/12).

115 See, for example, *Király and Dömötör v Hungary* App No 10851/13.

116 *Király and Dömötör v Hungary* App No 10851/13.

117 *Király and Dömötör v Hungary* App No 10851/13 at [41] - [43].

2.91 Furthermore, where an abusive communication interferes with the right to respect for private life, the State's positive obligations under Article 8 may include measures to restrict that communication, potentially by way of the criminal law.

2.92 This will not always be the case. The Court has contrasted cases of serious physical violence, which tend to require effective criminal law mechanisms, with cases of psychological harm, for which the same is not always true:

> as far as concerns less serious acts between individuals which may cause injury to someone's psychological well-being, the obligation of the State under Article 8 to maintain and apply in practice an adequate legal framework affording protection does not always require that an efficient criminal-law provision covering the specific act be in place. The legal framework could also consist of civil-law remedies capable of affording sufficient protection.[118]

2.93 In some cases, though, abusive communications interfering with the right to private life have been held to be sufficiently serious to require a response from the criminal justice system:

> the Court has examined under Article 8 the State's obligation to protect, for example, a minor against malicious misrepresentation…[119] The act in that case did not involve any physical violence, but could not be considered trivial as it entailed a potential threat to the minor's physical and mental welfare, brought about by the impugned situation, namely, that he was made the target for approaches by paedophiles. The act constituted a criminal offence under domestic law and the Court considered that practical and effective protection of the applicant required the availability of a remedy enabling the actual offender to be identified and brought to justice.[120]

2.94 Therefore, the positive obligation imposed by Article 8 may favour the restriction of expression by way of criminal offences in some circumstances. This potentially brings Article 8 and Article 10 into tension. In such circumstances, the Court's approach has been to conduct a balancing exercise.

### Balancing Article 8 and Article 10

2.95 In circumstances where one person's right to respect for private life under Article 8 has apparently been infringed by another person's exercise of their right to freedom of expression under Article 10, the Court must conduct a balancing exercise in respect of the two rights:

> where the complaint is that rights protected under art.8 have been breached as a consequence of the exercise by others of their right to freedom of expression, due regard should be had, when applying art.8, to the requirements of art.10 of the Convention. Thus, in such cases the Court will need to balance the applicant's right to "respect for his private life" against the public interest in protecting freedom of

---

118 *Noveski And Others v The Former Yugoslav Republic of Macedonia* App No 25163/08 at [61].

119 *K U v Finland* (2009) 48 EHRR 52 (App No 2872/02).

120 *Söderman v Sweden* (2014) 58 EHRR 36 (App No 5786/08) at [84].

expression, bearing in mind that no hierarchical relationship exists between the rights guaranteed by the two articles.[121]

2.96 The Court undertook this balancing exercise in the case of *Perinçek v Switzerland.*[122] The Swiss courts convicted Mr Perinçek, a Turkish politician, of a criminal offence after he publicly expressed the view that the mass deportation and massacre of Armenians in the Ottoman Empire in 1915 and in subsequent years did not amount to genocide. The decision for the ECtHR was whether this conviction amounted to an unlawful interference with Mr Perinçek's Article 10 right to freedom of expression, taking account of the Article 8 rights of modern-day Armenians to respect for their ethnic identity.

2.97 The court found that the interference with Mr Perinçek's right to freedom of expression was disproportionate and unlawful. In reaching this decision, the Court took account of the following factors:

(1) the applicant's statements bore on a matter of public interest and did not amount to a call for hatred or intolerance;

(2) the context in which the statements were made had not been marked by heightened tensions or special historical overtones in Switzerland;

(3) the statements could not be regarded as affecting the dignity of the members of the Armenian community to the point of requiring a criminal law response in Switzerland;

(4) there was no international law obligation for Switzerland to criminalise such statements;

(5) the Swiss courts appeared to have censured the applicant simply for voicing an opinion that diverged from the established ones in Switzerland; and

(6) the interference with his right to freedom of expression had taken the serious form of a criminal conviction.[123]

2.98 Decisions of the ECtHR tend to be highly fact-sensitive, and this case is no exception. However, these factors are instructive in considering the circumstances under which an interference with Article 10 may be considered disproportionate, even taking account of a countervailing Article 8 right. It seems clear that the Court will be attuned to some factors that are of general application: whether the exercise of freedom of expression concerned a matter of public interest; the context in which the impugned expression took place; and the gravity of the interference. Interferences in the form of a criminal conviction will, perhaps unsurprisingly, be more difficult to justify.

---

121 *Aksu v Turkey* (2013) 56 EHRR 4 (App No 4149/04) at [63].

122 *Perinçek v Switzerland* (2016) 63 EHRR 6 (App No 27510/08).

123 *Perinçek v Switzerland* (2016) 63 EHRR 6 (App No 27510/08) at [280].

## CONCLUSION

2.99 Articles 8 and 10 of the ECHR provide important limitations on the lawful, and legitimate, criminalisation of communications – whether online or otherwise. Yet, Article 8 may in some cases place the State under a positive obligation to restrict communications that interfere with the interests protected under Article 8(1). The provisional proposals in this Consultation Paper aim to ensure that the communications offences in England and Wales are compatible with the State's negative obligations under Article 10, and the State's positive and negative obligations under Article 8.

# Chapter 3: The existing law

## INTRODUCTION

3.1 In our Scoping Report,[124] we evaluated the existing criminal law covering abusive and offensive online communications. We concluded that the current patchwork of offences under-criminalises in some areas (by failing to proscribe certain forms of harmful behaviour) and over-criminalises in others (such that certain harmless or protected communications risk being caught within its scope). More generally, we found that the existing law is not always effective in targeting and labelling online abuse. In addition, some offences suffer from vagueness, leading to uncertainty and contributing to the problem of over-criminalisation. While there are criminal offences suitable for covering some types of abusive online communication – such as cyber-stalking and cyber-harassment – there remain practical and cultural barriers[125] to enforcement.

3.2 As we explained in the Introduction, following the Scoping Report, the Law Commission is currently working on two additional projects which are separate from, though related to, this Consultation Paper: one project is about the taking, making and sharing of intimate images without consent (the "image-abuse project") and the other project is about hate crime (the "hate crime project"). Some of the offences we looked at in the Scoping Report – including the stirring up hatred offences and voyeurism offences – are being reviewed as part of those projects.

3.3 The offences with which this Consultation Paper is primarily concerned are section 1 of the Malicious Communications Act 1988 ("MCA 1988") and section 127 of the Communications Act 2003 ("CA 2003"). These can be described as "general" communications offences, to be contrasted with more specific offences covering indecent and obscene communications.

3.4 In this chapter, we look first at the specific communications offences. These offences are limited in that they address only a narrow subset of online abuse. We do not, therefore, consider that they are appropriate vehicles for reform aimed at adequately addressing the full range of abusive online communications with which we are concerned. Given the full treatment of these offences in the Scoping Report, our analysis in this chapter is brief. It is intended to serve as a summary, with the purpose of explaining why these offences are not the main target of our proposals for reform.

3.5 Second, we consider the harassment and stalking offences under the Protection from Harassment Act 1997 ("PHA 1997"). In our view, the offences set out in the PHA 1997 adequately cover, at least in theory, the types of abusive behaviours they seek to address, including the online forms of such behaviours. That being said, the complicated drafting of some of these offences sometimes leads to

---

[124] Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381.

[125] Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 3.12. We outline these barriers below, at para 1.58.

misunderstandings and, partly as a result of this lack of clarity, the offences are not always used in practice. In addition to these problems, there is a gap in the protection afforded by the PHA 1997 as against uncoordinated group (or "pile-on") harassment.

3.6 Finally, we look at the general communications offences. Given their broader scope, we consider that the general communications offences are more suitable candidates for reform. In this chapter, we explain in detail the problems with these offences, which justify, at least in part, the provisional proposals for reform that we make in Chapter 5.

## SPECIFIC OFFENCES: OBSCENE AND INDECENT COMMUNICATIONS

3.7 There are a variety of specific offences covering obscene and indecent communications, including some online communications. These are:

(1) the common law offence of outraging public decency;

(2) offences under the Indecent Displays (Control) Act 1981; and

(3) offences under the Obscene Publications Act 1959.

3.8 In this section we explain why, in our view, these offences are too narrow adequately to address the full range of abusive online communications with which we are concerned.

### Outraging public decency

3.9 The common law offence of outraging public decency[126] is composed of the following elements:

(1) the defendant carried out an act of lewd, obscene or disgusting character that outrages minimum standards of public decency;

(2) the act took place in a public place, or a place which is accessible to, or within view of, the public; and

(3) the act took place in the actual presence of two or more persons who were capable of seeing it, whether or not anyone actually saw it or was outraged by it (the "two-person rule").

---

[126] The Law Commission has previously made recommendations as to reform of this offence. See: Simplification of Criminal Law: Public Nuisance and Outraging Public Decency (2015) Law Com No 358. We recommended making outraging public decency a statutory offence. Our recommended offence would require that an act or display be obscene or disgusting, to an extent sufficient to outrage minimum standards of public decency as judged by the jury in contemporary society. It would retain a requirement that the act or display must be in a place which is accessible to or within view of the public. It would not include the "two-person rule". It would also have a fault element (the defendant knew of the nature of that act or display, or was reckless as to whether the act or display was of that nature; and knew or intended that the act or display was or would be in a place which is accessible to or within view of the public, or was reckless as to whether or not this was the case) and a reasonableness defence.

3.10 The requirements of this offence make it too narrow usefully to address online communications which warrant criminalisation.[127] This is for three main reasons: first, not all websites or platforms are obviously public in nature. Twitter might be an example of a relatively public platform, where there is very little restriction on the ability of anyone to view messages posted on the platform. However, Facebook may not constitute a public place, especially where the user's security settings limit the visibility of a post to a select group of viewers.

3.11 Second, all three requirements must be met at the same time. It is not sufficient that, having been recorded, the act was viewed subsequently. It may well be that, for popular platforms, the two-person rule is met when the act is carried out. But in a less popular public forum – such as, perhaps, the comments section beneath a news article – it may be that no one is present when the act is carried out. This will be the case even if the offending communication is subsequently viewed by many people.[128]

3.12 Third, and perhaps most fundamentally, this offence covers only lewd, obscene or disgusting communications that outrage minimum standards of public decency. Hence, it is too narrow to address the various online communications and harms with which we are concerned. This kind of problem is, in our provisional view, common to all of the specific communications offences considered in this section.

### Indecent Displays (Control) Act 1981

3.13 Section 1(1) of the Indecent Displays (Control) Act 1981 makes it an offence to display publicly any "indecent matter". The offence is as follows:

> (1) 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.
>
> (2) Any matter which is displayed in or so as to be visible from any public place shall, for the purposes of this section, be deemed to be publicly displayed.

3.14 The Act contains two exemptions from the definition of "public" which make it too narrow for the online sphere. First, section 1(3)(a) excludes from the definition of "public" any places that the public must pay to access. Therefore, a significant range

---

127 *R v Hamilton* [2007] EWCA Crim 2062, [2008] QB 224. Mr Hamilton engaged in "up-skirting" using a camera that was mostly, but not entirely, concealed in a rucksack. He was convicted of the offence of outraging public decency. The Court held that one of the elements of the offence is that the activity took place in a public place and must have been capable of being seen by two or more persons who were actually present, even if they had not actually seen it. In this case, there was evidence from the videos that others were present. No one actually saw Mr Hamilton filming; however, the Court found that his filming was capable of being seen. Since April 2019, this behaviour has also been criminalised under section 67A of the Sexual Offences Act 2003 (the new "up-skirting" offence). We are considering potential reform of this offence, and other intimate image offences, as part of our project on the taking, making and sharing of intimate images without consent.

128 The statutory offence we recommended in our report, Simplification of Criminal Law: Public Nuisance and Outraging Public Decency (2015) Law Com No 358, would represent some improvement in this regard, in that it would not include the "two-person rule". However, it would retain a requirement that the act or display must be in a place which is accessible to or within view of the public. Hence, our recommended offence, like the existing common law offence, would be unsuitable for addressing many forms of online communication.

of online activity would fall outside the scope of the offence (comments on news articles behind a paywall, messaging services in certain games or mobile applications, etc).

3.15 Second, section 1(3)(b) further exempts those places in shops that can only be accessed after passing a warning notice. It is not clear whether this might be interpreted purposively so as to include online spaces that contain written warnings. Given that the exemption specifically refers to "shops", it must be considered that this would not apply automatically to online spaces. Nonetheless, it remains a possibility that adequate warning pages could ensure that communications thereafter fall outside the scope of the offence.

3.16 In any case, the legislation only covers material that is indecent; this is a law which was intended to restrict the visibility of sexually explicit material,[129] albeit that there is no definition of "indecent" in the legislation, nor has any additional clarification been provided.[130] Hence, here again, the offence is too narrow to address the various online communications and harms with which we are concerned.

3.17 Finally, we noted in the Scoping Report that, according to internal case management data provided by the CPS, there were no prosecutions under this legislation between 2015 and 2018 and in each of 2014 and 2015 just one charge was authorised.[131] This is a strong indication that the offence is too narrow to cover abusive online communications, which, as we explained in the Scoping Report and reiterate in Chapter 4, are sent and received on an enormous scale.

### Obscene Publications Act 1959

3.18 The Obscene Publications Act 1959 makes it an offence to publish an "obscene article" or to possess, own or control an "obscene article" for publication for gain.[132] Under section 2 of the Act, 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).

3.19 One problem with this offence is the definition of "obscene". The test for obscenity is contained in section 1(1) of the Act but is derived from the common law "*Hicklin* principle", under which obscenity is defined as a tendency to "deprave and corrupt those whose minds are open to… immoral influences".[133] The statute modified this definition such that an article is obscene if it has a tendency to deprave and corrupt those who are "likely, having regard to all relevant circumstances, to read, see or

---

129 M Childs, "Outraging public decency: the offence of offensiveness" [1991] *Public Law* 20.

130 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 6.93.

131 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 6.96.

132 Obscene Publications Act 1959, ss 1 and 2.

133 *R v Hicklin* (1868) LR 3, QB 360, 371.

hear" the relevant material. As we noted in the Scoping Report, this makes the offence "context-dependent".[134]

3.20 In the Scoping Report we observed that this test, requiring consideration of the likely effect on likely viewers, raises particular challenges in relation to online communications. Often, material "published" on the internet, particularly material posted on social media or on a website, is, potentially accessible to anyone - including "vulnerable young people", as noted in *R v Perrin.*[135] This presents a risk of over-criminalisation, since some material published on the internet might too easily meet the statutory test.

3.21 Problems also arise in an online context regarding the definitions of "article" and "publication". In *R v Smith,* the Act was used to prosecute the defendant for sending messages to another (unidentified) individual that discussed explicit, sadistic and incestuous sexual acts on young children.[136] The "articles" were these comments and statements, and the "publication" was communication of these to one other, unidentified person. As we noted in the Scoping Report, academics such as Alisdair Gillespie have argued that this decision is an over-broad application of the Act, which goes beyond what Parliament intended. According to Gillespie, "the OPA 1959 was never intended to regulate private communications and there is no reason for it to stray into this area".[137] 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 communications rather than publications. At present, *Smith* seems to be an isolated example of a prosecution under the Act where the conduct was one-to-one online messaging.

3.22 Finally, like the other specific communications offences discussed above, the Obscene Publications Act 1959 is too narrow to capture the various online communications and harms with which we are concerned. Given the fundamental requirement that material must be "obscene", it simply cannot provide a solution in all cases. There are many types of harmful online communication which ought to be criminalised, but which could not plausibly be described as "obscene" (consider, for example, a threat).

3.23 In short, we do not consider that any of the specific communications offences discussed in this section are appropriate vehicles for reforms aiming to address online abuse.

---

134 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381at para 6.18, quoting J Jaconelli, "Context-Dependent Crime" [1995] *Criminal Law Review* 771.

135 [2002] EWCA Crim 747 at [22].

136 [2012] EWCA Crim 398, [2012] 1 WLR 3368.

137 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381at [6.65], referencing A Gillespie, "Obscene conversations, the internet and the criminal law" [2014] *Criminal Law Review* 350, at p 363.

## HARASSMENT AND STALKING OFFENCES

3.24 Much broader than the specific communications offences discussed above are the stalking and harassment offences.

3.25 Neither harassment nor stalking has a clear and consistent legal definition, though definitions do appear in non-criminal legal contexts, such as anti-discrimination and employment law.[138] In case law, it has been suggested that the terms "harassment" and "stalking" are "generally understood".[139] One of the key features of stalking and harassment is that they involve a "course of conduct", rather than a one-off communication.

3.26 As we explain in the Scoping Report, the online environment, with its incredible connectivity, has facilitated new forms of stalking and harassment. Internet technology gives perpetrators an array of new access points to victims. New forums of stalking and harassment include dating apps[140] and online gaming sites.[141] Stalking, in particular, is facilitated by, for example, spyware and smart home technology.[142]

3.27 At least in principle, the stalking and harassment offences offer effective protection against these new forms of online abuse. In this section, we set out: the various stalking and harassment offences; their strengths; and their problems and limitations.

### Protection from Harassment Act 1997

3.28 As we explain in the Scoping Report, the behaviours of stalking and harassment are criminalised primarily under the PHA 1997. This Act covers harassment perpetrated by one person against another and has evolved to include harassment perpetrated by and against groups.

#### The offence of harassment

3.29 Under the PHA 1997, the offence of harassment is a summary only offence carrying a maximum penalty of six months' imprisonment or a fine.[143] The offence is set out at section 1(1) of the Act:

> A person must not pursue a course of conduct—
>
> (a) which amounts to harassment of another, and

---

138 See Equality Act 2010, s 26.

139 *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233, [2002] Entertainment and Media Law Reports 4 at [30].

140 See, for example, L Thompson, ""I can be your Tinder nightmare": Harassment and misogyny in the online sexual marketplace" (2018) 28(1) *Feminism and Psychology* 69.

141 See, for example, Ditch the Label, *In Game Abuse* (2017), https://www.ditchthelabel.org/research-papers/ingame-abuse/ (last visited 07 September 2020).

142 See, for example, J Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity" (2019) 15(1) *St Antony's International Review* 83. For further detail on these kinds of online abuse, see Chapter 4.

143 Protection from Harassment Act 1997, s 2(2).

(b) which he knows or ought to know amounts to harassment of the other.

3.30 Section 7 of the Act provides that "harassing a person" includes "alarming the person or causing the person distress". The Court of Appeal in *Thomas v News Group Newspapers* further defined the term "harassment":

> 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.[144]

3.31 Therefore, 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".[145]

3.32 The offence requires a "course of conduct" amounting to harassment. Under section 7(3)(a) a "course of conduct" must involve "in the case of conduct in relation to a single person … conduct on at least two occasions in relation to that person". However, as we explain in the Scoping Report, there need only be one effect of the defendant's course of conduct, namely, that the victim is harassed. Therefore, conduct not initially experienced as harassment by the victim may nonetheless form part of the course of conduct if the cumulative effect is that the victim is harassed.[146]

3.33 Under section 1(3), a defendant has a defence if they can show in relation to a course of conduct:

(a) that it was pursued for the purpose of preventing or detecting crime,

(b) that it was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under any enactment, or

(c) that in the particular circumstances the pursuit of the course of conduct was reasonable.

### Harassment perpetrated by a group ("coordinated harassment")

3.34 In addition to the individual offence, there is a group harassment offence under section 7(3A) of the PHA 1997, which provides:

> A person's conduct on any occasion shall be taken, if aided, abetted, counselled or procured by another—

---

144 *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233, [2002] Entertainment and Media Law Reports 4 at [30].

145 *Majrowski v Guy's and St. Thomas' NHS Trust* [2006] UKHL 34, [2007] 1 AC 224 at [30].

146 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 8.38.

(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.

3.35 The drafting is complex, but ultimately it means that the "course of conduct" can be completed by two individual acts by two different defendants so long as the first defendant aided, abetted, counselled or procured the conduct of the second defendant. This kind of conduct can be described using the shorthand "coordinated harassment".

3.36 In theory, then, harassment perpetrated by a group can be prosecuted under the PHA 1997. As we explain in the Scoping Report, this means that if, for example, the first defendant sent a harassing email to a victim, and then helped three other defendants to draft harassing emails which each of them individually sent to the victim, then the first defendant could be liable for harassment. By virtue of section 7(3A), the harassing emails sent by the other three defendants are deemed to be part of the first defendant's course of conduct. This is because the first defendant aided (or abetted or counselled or procured) the conduct of the other three.

### Harassment perpetrated against a group

3.37 There is also an offence of harassment of two or more persons by virtue of section 1(1A), added in 2005.[147] The offence 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 under no obligation to do.

3.38 It should be noted that this form of harassment involves an additional fault element, as compared to the basic offence: the defendant must intend to persuade someone to do or not to do something.

3.39 This offence can be used to protect, for example, families or religious groups from harassment.

---

147 Inserted by section 125(2)(a) of the Serious Organised Crime and Police Act 2005.

### The offence of stalking

3.40 As the Court of Appeal made clear in *Thomas v News Group Newspapers,* harassment has always included stalking: stalking was given as a "prime example" of harassing conduct.[148] Stalking was, however, introduced as a specific offence by the Protection of Freedoms Act 2012.[149]

3.41 The offence of stalking has the same elements as the offence of harassment, with the additional element that the acts or omissions that constitute the course of conduct must be ones associated with stalking.[150]

3.42 Section 2A(3) of the PHA 1997 provides a non-exhaustive list of acts and omissions that may be associated with stalking:

(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 that 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.

## Strengths of the stalking and harassment offences

3.43 One of the main strengths of the stalking and harassment offences for the purposes of this discussion is that they are sufficiently broad and flexible to include many forms of online abuse. In addition, the criminal offences are buttressed by a variety of other mechanisms for protecting victims. We discuss these strengths below.

### Breadth and flexibility

3.44 At least in principle, the offences of harassment and stalking apply online as they do offline. A "course of conduct" could include online communications such as emails, Tweets, or liking or tagging online content. Recent cases of relevance include, for

---

148 *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233, [2002] Entertainment and Media Law Reports 4 at [30].

149 Protection of Freedoms Act 2012, s 111.

150 Protection from Harassment Act 1997, s 2A(2).

example, *Khan v Khan,*[151] in which the defendant sent around 70 harassing emails over a period of around nine months.

3.45 Emailing and other forms of direct communication with the victim are, perhaps, the more obvious examples of online harassment. However, the offences under the PHA 1997 are capable of covering a wide variety of harmful online behaviours, some of which do not necessarily take the form of direct communication. In the Scoping Report, we enumerated some examples of conduct that courts have held to constitute harassment. These include, for example, posting or threatening to post private information about the victim on the internet (otherwise known as "doxing"), deemed to be harassment in the case of *WXY v Gewanter.*[152] It also includes surveillance in an attempt to prove that an individual was committing benefit fraud: *Howlett v Holding*.[153] Following the logic of *Howlett v Holding*, our view is that harassment could encompass cyber-surveillance and other forms of tech-enabled abuse, though we have not been able to find any cases directly on point.

3.46 In addition, the list of acts and omissions which may be associated with stalking in section 2A(3) PHA 1997 includes a range of behaviours, some of which can clearly be perpetrated online. For example, "monitoring a person's use of the internet or email" is likely itself to take place using internet technology.

3.47 Further, "watching or spying" is now enabled by, for example, smart home devices or spyware and disproportionately affects women and girls.[154] The CPS *Guidelines on prosecuting cases involving communications sent via social media* acknowledge that this is the case:

> The use of the internet, social media platforms, emails, text messages, smartphone apps (for example, WhatsApp; Snapchat), spyware and GPS (Global Positioning System) tracking software to commit VAWG [violence against women and girls] offences is rising.[155]

3.48 The CPS guidance helps to clarify the many forms of online activity that may constitute stalking. In addition to direct forms of online communication (such as emails or WhatsApp messages sent directly from the perpetrator to the victim), the CPS guidance lists various other examples of cyberstalking. These include:

(1) "baiting" or humiliating peers online by labelling them as sexually promiscuous;

---

151 *Khan v Khan* [2018] EWHC 241 (QB).

152 *WXY v Gewanter* [2012] EWHC 496 (QB).

153 *Howlett v Holding* [2006] EWHC 41 (QB), (2006) 150 Solicitors Journal Law Brief 161.

154 For discussion see, for example, J Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity" (2019) 15(1) *St Antony's International Review* 83.

155 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (last revised 21 August 2018), https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (last visited 07 September 2020).

(2) unwanted indirect contact with a person that may be threatening or menacing, such as posting images of that person's children or workplace on a social media site, without any reference to the person's name or account;

(3) posting photoshopped images of persons on social media platforms;

(4) hacking into social media accounts and then monitoring and controlling the accounts;

(5) sending electronic viruses; and

(6) cyber identity theft.[156]

3.49 In short, it seems clear that the offences of harassment and stalking cover, at least in principle, a wide range of abusive online behaviour.

### Mechanisms for protecting victims: Stalking Protection Orders

3.50 Another advantage of the stalking and harassment offences is the range of related mechanisms available to protect victims, aside from criminal prosecution. As we explain in the Scoping Report, these include injunctions under section 3 of the PHA 1997. These are civil orders which do not require criminal prosecution. They apply in circumstances of "actual or apprehended harassment". A breach of a civil injunction under the PHA 1997 carries a maximum penalty of five years' imprisonment.[157]

3.51 Since 20 January 2020 these protective mechanisms have also included Stalking Protection Orders ("SPOs"), introduced by the Stalking Protection Act 2019 and accompanied by detailed statutory guidance.

3.52 For these purposes, the CPS and police have adopted the following definition of stalking: "a pattern of unwanted, fixated and obsessive behaviour which is intrusive. It can include harassment that amounts to stalking or stalking that causes fear of violence or serious alarm or distress in the victim".[158]

3.53 Like the injunctions relating to harassment, an SPO is a civil order. The order is made on application by the police to the magistrates' court. Under section 1(1) of the SPA 2019, a chief officer of the police may apply for an SPO if it appears to the chief officer that:

(a) the defendant has carried out acts associated with stalking,

(b) the defendant poses a risk associated with stalking to another person, and

---

156 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (last revised 21 August 2018), https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (last visited 07 September 2020).

157 Protection from Harassment Act 1997, s 3(9).

158 Crown Prosecution Service, *Guidance on Stalking Protection Orders* (20 January 2020), https://www.cps.gov.uk/legal-guidance/stalking-protection-orders (last visited 07 September 2020).

(c) there is reasonable cause to believe the proposed order is necessary to protect another person from such a risk (whether or not the other person was the victim of the acts mentioned in paragraph (a)).

3.54 The power of the police to apply for an SPO is intended to minimise burdens on the victim.[159] From the perspective of adequately protecting victims, this is a significant advantage.

3.55 SPOs were introduced as part of the Government's wider initiatives to tackle violence against women and girls: the Crime Survey for England and Wales 2019 reported that more than 1 in 5 women aged 16 to 59 have been victims of stalking, compared to nearly 1 in 10 men.[160] While SPOs can apply to any case of stalking, they are designed specifically to tackle so-called "stranger stalking", which does not take place in the context of domestic abuse, but by a perpetrator not previously known to the victim.

3.56 Although it is too early to assess their effectiveness, organisations such as the Suzy Lamplugh Trust have welcomed the introduction of SPOs.[161]

### Problems with the stalking and harassment offences

3.57 Notwithstanding the strengths outlined above, there are problems with the stalking and harassment offences. First, there is a significant gap in the protection afforded by the PHA 1997: the offences do not adequately cover uncoordinated group harassment (see further the discussion below). In addition, despite the theoretical ability of the PHA 1997 to cover adequately a range of online abuse there are, as we noted in the Scoping Report, significant practical and cultural barriers to enforcement. We discuss these problems below.

#### Practical and cultural barriers to enforcement

3.58 As we explain in the Scoping Report, practical and cultural barriers to enforcement of criminal offences relating to online abuse include:

(1) the scale of abusive and offensive online communications and the limited resources that law enforcement agencies and prosecutors have available to pursue these;

---

159 See, for example, Home Office and Victoria Atkins MP, *Government backed Stalking Protection Bill receives Royal Assent* (15 March 2019), https://www.gov.uk/government/news/government-backed-stalking-protection-bill-receives-royal-assent (last visited 07 September 2020).

160 Home Office and Victoria Atkins MP, *Government backed Stalking Protection Bill receives Royal Assent* (15 March 2019), https://www.gov.uk/government/news/government-backed-stalking-protection-bill-receives-royal-assent (last visited 07 September 2020), citing National Office for Statistics, *Crime Survey for England and Wales* (2018), https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018 (last visited 07 September 2020).

161 Suzy Lamplugh Trust, *Stalking Protection Orders* (18 February 2020), https://www.suzylamplugh.org/News/stalking-and-protection-orders (last visited 07 September 2020).

(2) persistent cultural tolerance of online abuse, which means that even when reported, it is not always treated as seriously as offline conduct;

(3) technical barriers to the pursuit of online offenders, such as tracing and proving the identity of perpetrators, and the cost of doing so; and

(4) jurisdictional and enforcement barriers arising from the globalised nature of the online environment.[162]

3.59 Compared with the general communications offences (section 1 of the MCA 1988 and section 127 of the CA 2003, discussed below), the stalking and harassment offences are prosecuted frequently. In 2018–19, there were 10,636 stalking and harassment offences prosecuted, of which 2,209 were stalking offences.[163] In 2017–18, there were 11,922 stalking and harassment prosecutions.[164]

3.60 However, there is no recorded data to distinguish the proportion of prosecutions relating to conduct that took place solely or partially online. Anecdotally, a consistent message from stakeholders has been that harassment and stalking that takes place online is often taken less seriously by enforcement agencies than equivalent conduct that takes place offline. For example, Report Harmful Content ("RHC") – a national reporting centre for harmful online content, provided by the UK Safer Internet Centre and operated by South West Grid for Learning – in their *Pilot Year Evaluation Report* recently found that:

> One particularly concerning issue arose regarding law enforcement. 19% of RHC clients reported content which was deemed to be criminal and thus referred to law enforcement. Of that 19%, however, 47% got back in touch with RHC, often reporting that the police had dismissed them and incorrectly informed them that their issue was non-criminal. These findings thus support previous recommendations regarding the need for better training of law enforcement on issues of online crime and abuse.[165]

3.61 These problems are compounded by the complex drafting of the PHA 1997. This is particularly true of section 7(3A) which, as we noted in the Scoping Report, seems rarely if ever to be prosecuted.[166] It may be regarded as disproportionate for limited

---

162 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381 at para 13.12.

163 Crown Prosecution Service *Violence Against Women and Girls Report 2018–19*, at A15, https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2019.pdf (last visited 07 September 2020).

164 The combined total for prosecutions under section 1 of the MCA 1988 and section 127 of the CA 2003 was, in 2018–19, 5,952.

165 Report Harmful Content, *Pilot Year Evaluation* (2020), https://d1afx9quaogywf.cloudfront.net/sites/default/files/RHC%20Report%20Final%20with%20Logos_0.pdf (last visited 07 September 2020).

166 Section 7(3A) of the PHA 1997 was considered in the civil case of *Hourani v Thomson* [2017] EWHC 432 (QB), concerning a "campaign" of harassment against Mr Hourani orchestrated by several defendants. Mr Justice Warby rejected the argument made by one of the defendants that, since they had engaged in only one instance of conduct, they had not engaged in harassment. Mr Justice Warby found, at [136], that the conduct of the other co-defendants could be attributed to the defendant pursuant to section 7(3A), because he aided and abetted that conduct.

resources available for pursuing online abuse to be devoted to charges based on complex but at the same time low-level offences.

3.62 Such problems are significant. However, they do not, for the most part, lie with the letter of the law and are not likely to be solved by changes to the offences themselves. Instead, solutions might include:

(1) extra training to ensure that police are better able to recognise stalking and harassing behaviours, especially when such behaviours are perpetrated online;

(2) public education to help address minimisation and tolerance of online stalking and harassing behaviours; and

(3) specialist intervention programmes for perpetrators of stalking and harassment, which could work in conjunction with SPOs to reduce offending behaviour.

### Gaps in protection

3.63 A significant gap in the protection afforded by the PHA 1997 is that it does not cover uncoordinated group (or "pile-on") harassment. Pile-on harassment occurs when many individuals, acting separately, send messages that are harassing in nature to a victim. For example, hundreds of individuals sent messages to Jess Phillips MP along the lines of "I would not rape you".[167] This phenomenon is relatively unique to the online environment.

3.64 As we noted in our Scoping Report, the criminal law is currently ineffective when it comes to dealing with this kind of situation, where a single person sends a single abusive message:

(1) in the knowledge that similar abuse is being targeted at the victim; and

(2) with an awareness of the risk of greater harm to the victim occasioned by their conduct in the circumstances.[168]

3.65 Lacking explicit coordination, these messages do not constitute a course of conduct for the purposes of section 7(3A) of the PHA 1997, despite the fact that the experience of the victim may be identical to, or worse than, more formally coordinated harassment.

3.66 Given this gap in protection afforded by the PHA 1997, in Chapter 6 we give detailed consideration to pile-on harassment and make proposals for reform specifically to address this phenomenon.

---

[167] See, for example, M Oppenheim, *Labour MP Jess Phillips receives '600 rape threats in one night'* (31 May 2016), https://www.independent.co.uk/news/people/labour-mp-jess-phillips-receives-600-rape-threats-in-one-night-a7058041.html (last visited 07 September 2020).

[168] Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 8.207.

## PUBLIC ORDER OFFENCES

### Public Order Act 1986

3.67 The Public Order Act 1986 ("POA 1986") contains a range of offences which can apply to abusive or threatening behaviour online, particularly under sections 4, 4A and 5 (as to which see below). However, these offences were not designed to address online behaviour and applying them online in their current forms presents some real challenges.

3.68 For example, none of the offences can 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".[169] This is a significant limitation. It is, of course, common for online interaction to take place between people in their homes. This requirement – as with the public communications network requirement in the CA 2003 (see the discussion below) – arbitrarily restricts the usefulness of these offences in addressing threatening behaviour online.

3.69 Further, the existence of the "dwellings exemption" reflects the clear intent of the lawmakers that public order offences should, as the name suggests, criminalise behaviour committed in public spaces. In our Scoping Report, we cited a number of academics who argued that the conceptual underpinnings of the offences – and the considerations that informed their structure – are not a neat fit with the nature of behaviour and harm in digital spaces. As David 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".[170] John 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".[171]

3.70 This latter point can be seen in some of the rationale for public order legislation. The law of public order has been described as being "often made to reflect its time".[172] The 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 football disorders in the 1980s, which preceded the Public Order Act

---

169 A "dwelling" is defined in section 8 of the POA 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.

170 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), at p 1.

171 J E Stannard, "Sticks, Stones and Words: Emotional Harm and the English Criminal Law" (2010) 74(6) *Journal of Criminal Law* 533, at p 543.

172 HHJ P Thornton and others, *The Law of Public Order and Protest* (2010), at p v.

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.[173]

3.71 Jacob Rowbottom's observation that we cited in our Scoping Report bears recalling here:

> 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 a different impact on the listener. That is what makes public 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.[174]

3.72 We address these offences and their limitations in turn.

### Section 4 of the Public Order Act 1986: fear or provocation of violence

3.73 Under section 4(1) of the POA 1986 a person is guilty of an offence if they:

> (a) use towards another person threatening, abusive or insulting words or behaviour; or
>
> (b) 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.

3.74 The offence has a number of limitations. First, the offence can only be committed "towards another".[175] In *Atkin v DPP*[176] 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.

3.75 Second, the fault element has two parts, both of which must be met. The first element is that the defendant either intends their words or behaviour to be threatening,

---

173 *Hansard* (HC), 13 January 1986, vol 89, col 795 (Mr Douglas Hurd, Secretary of State for the Home Department).

174 J Rowbottom, "To rant, vent and converse: protecting low level digital speech" 71(2) *The Cambridge Law Journal* 355, at p 361.

175 However, it seems that it is not necessary for that person to be called to give evidence. See, for example, *Swanston v DPP* (1997) 161 JP 203, where the prosecution relied on evidence from a bystander.

176 (1989) 89 Cr App R 199.

abusive, or insulting, or is aware that they may be.[177] Second, the defendant must intend a specific reaction to their words or behaviour, relating to the use of unlawful violence. Together, these two elements set a high threshold and mean that the offence can only address a narrow subset of abusive online behaviour.

3.76 Third, the dwelling exemption applies to this offence (as with the other POA offences): 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".

3.77 Fourth, the apprehension or provocation must be as to the *immediate* use of violence. The immediacy of the unlawful violence is a question of fact. However, while there is some disagreement as to the necessary proximity of the threat, it seems clear that much threatening behaviour online would fall outside the scope of this offence. In *R v Horseferry Road Metropolitan Stipendiary Magistrates ex parte Siadatan*[178] 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.[179]

3.78 In *DPP v Ramos*,[180] two letters to an Asian community advice centre threatening the start of a bombing campaign and the murder of the recipient was held to constitute 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".[181] Provided, therefore, the victim believed and was likely to believe that something could happen at any time, there was a case to answer.

3.79 This decision has been criticised, most notably by Professor 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 was open to him to infer than they feared immediate violence

177 Public Order Act 1986, s 6(3).

178 [1991] 1 QB 260.

179 [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.

180 [2000] *Criminal Law Review* 768.

181 *DPP v Ramos* [2000] All ER (D) 544 at [10].

> …[this] is very far removed from the traditional examples of assault where the victim flinches from the upraised fist, the drawn sword or the charging horse.[182]

3.80 Fifth, the communication must, of course, be "threatening, abusive or insulting". As we discuss in the following chapter, we do not consider that these categories adequately track all conduct which ought to be proscribed. What constitutes "threatening, abusive or insulting" is also a question of fact. Lord Reid said in *Brutus v Cozens*:[183]

> 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.[184]

3.81 Finally, the defendant will only be guilty under section 4 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.[185]

### Section 4A of the Public Order Act 1986: intentional harassment, alarm or distress

3.82 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 he or she:

> (a) uses threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
>
> (b) displays any writing, sign or other visible representation which is threatening, abusive or insulting,
>
> thereby causing that or another person harassment, alarm or distress.

3.83 The offence shares many of the limitations of section 4. First, the dwelling exemption applies (section 4A(3)). Second, there are prescribed categories of behaviour that do not necessarily track the harmful behaviour we consider in the following chapter.

3.84 Of particular note in the section 4A offence is the requirement that someone actually suffers harassment, alarm or distress. 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".[186] While the person who suffered that distress does not necessarily have to have seen the writing or image,[187] requiring proof of such distress provides an obstacle to prosecution which, as we

---

182 JC Smith, "Public order offence: respondent sending letters stating an intention to arrange a bombing hate campaign" [2000] *Criminal Law Review* 768, at p 769.

183 [1973] AC 854 at 862.

184 *Brutus v Cozens* [1973] AC 854 at 862.

185 Public Order Act 1986, s 6(3).

186 *R(R) v DPP* [2006] EWHC 1375 (Admin), (2006) 170 JP 661 at [12].

187 *S v DPP* [2008] EWHC 438 (Admin), [2008] 1 WLR 2847 at [15] (Walker LJ).

argue in Chapter 5, may not be an unreasonable obstacle. In any case, the harm specified in this offence is of a particular kind and of a particular level of seriousness: in Chapter 5, we consider whether these offences are appropriate for addressing online behaviour.

### Section 5 of the Public Order Act 1986: harassment, alarm or distress

3.85 The offence under section 5 has fewer limitations than either sections 4 or 4A, though we still have reservations as to its effectiveness in addressing harmful online behaviour.

3.86 Under section 5(1) of the POA 1986, a person is guilty of an offence if he:

(a) uses threatening or abusive words or behaviour, or disorderly behaviour; or

(b) displays 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.

3.87 Prior to 2013, the offence also extended to "insulting" words. This language was removed following concern that this extended the reach of the offence too far.[188]

3.88 The offence does not require any violent behaviour or indeed the threat of violence. 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.

3.89 Unlike the section 4A offence, 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 did see or hear the threat.[189]

3.90 There are two ways in which a section 5 offence may be committed online: "using" threatening or abusive words or behaviour, or by "displaying" threatening or abusive words or signs.

3.91 In *Chappell v DPP*,[190] the Divisional Court agreed that the posting of a letter through a letterbox, where the writing containing the abusive or insulting words was inside and

---

188 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), http://researchbriefings.files.parliament.uk/documents/SN05760/SN05760.pdf (last visited 07 September 2020).

189 *Taylor v DPP* [2006] EWHC 1202 (Admin), (2006) 170 JP 485.

190 (1988) 89 Cr App R 82.

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 Twitter is probably "on display", but this may not be as straightforward if the message was sent using a private encrypted messaging service.

3.92 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 and more specific offences designed to deal with such threatening and abusive behaviour, which we discuss further in Chapter 5. 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, though Chara Bakalis has suggested that it rules section 5 out in application to threatening, abusive or disorderly behaviour online.[191]

3.93 Given the limitations of all three offences, we share the view of Nicola Haralambous and Neal Geach that the offences are of "questionable value for the social networking age", contributing "to the issues of uncertainty and inaccessibility of the overall legislative framework".[192]

## GENERAL COMMUNICATIONS OFFENCES

3.94 Like the offences under the Protection from Harassment Act 1997, the offences under section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003 are much broader than the specific communications offences considered above. They are capable of addressing a wide range of abusive online communications. In particular, they are capable of addressing one-off communications in a way that the stalking and harassment offences are not. However, they also suffer from some fairly serious problems.

3.95 Here we set out: the elements of these offences; their strengths; and their problems and limitations.

### Malicious Communications Act 1988

3.96 The Malicious Communications Act 1988 contains a general communications offence. Section 1 MCA 1988 provides that:

> (1) Any person who sends to another person –

---

191 C Bakalis, "Rethinking cyberhate laws, Information & Communications Technology Law" (2018) 27(1) *Information & Communications Technology Law* 86, at p 94. Bakalis notes that while sections 4 and 4A of the POA 1986 can in theory be applied to online conduct, their usefulness is limited.

192 N Haralambous and N Geach, "Regulating Harassment: Is the Law Fit for the Social Networking Age?" (2009) 73 *Journal of Criminal Law* 241, at p 256.

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

3.97 The offence under section 1(1)(a) can be broken down into the following elements:

(1) the defendant, sends a communication to an intended recipient;

(2) the communication is indecent or grossly offensive, a threat, or is false and is known or believed by the defendant to be false;

(3) the defendant intends to cause the victim distress or anxiety.

3.98 Online communications are covered by this offence. "A communication" is defined broadly. It includes "electronic communication" and, therefore, online communications.[193]

3.99 As we noted in the Scoping Report, there is no requirement that the communication be received by anyone. The offence is complete at the moment the communication is sent. So, if, for example, the defendant sends an email to an intended recipient but, due to a technical error, the email never reaches intended recipient's inbox, the defendant may nonetheless have committed an offence under section 1.

3.100 For context, in 2018-19 there were 3,358 offences charged under section 1; an increase from 3,079 in 2017-18.[194]

### Communications Act 2003

3.101 The Communications Act 2003 provides for other general communications offences. Section 127 provides that:

(1) A person is guilty of an offence if he—

---

193 Malicious Communications Act 1998, s 1(1)(a).

194 Crown Prosecution Service, *Annual Violence Against Women and Girls Report 2018-19*, p A53, https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2019.pdf (last visited 07 September 2020).

(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.

3.102 The offence under section 127(1) CA 2003 has the following elements:

(1) the defendant sends a message (or other matter) over a public communications network; and

(2) the message (or other matter) is grossly offensive, indecent, obscene, or menacing.

3.103 There is no requirement that the message (or other matter) be sent to anyone in particular or that it be received by anyone at all.

3.104 Under section 127(2) there is a further offence of sending false or persistent communications for the purpose of causing annoyance, inconvenience or anxiety to another.

3.105 For context, in 2018-19, there were 2,594 offences charged under section 127 (a decrease from 2,950 in 2017-18).[195] At present, section 127 is used to prosecute a variety of conduct, including not only abusive online communications but also hoax 999 calls and certain forms of cold-calling.

## STRENGTHS OF THE GENERAL COMMUNICATIONS OFFENCES

3.106 The general communications offences have certain strengths. In particular, their breadth and flexibility enables them to be used in a wide range of circumstances, making them a useful prosecutorial tool in tackling a variety of harmful behaviour, from low-level hate crime to domestic abuse.

3.107 According to internal data provided to us by the CPS, section 127(2) is most commonly used to prosecute hoax calls to the emergency services. Of a random sample of prosecutions brought under section 127(2), 17 out of 26 were of this type. In our view, section 127(2) therefore has a specific and useful function aside from the

---

195 Crown Prosecution Service, *Annual Violence Against Women and Girls Report 2018-19*, p A53, https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2019.pdf (last visited 07 September 2020).

prosecution of abusive communications. In Chapter 6, we make proposals for reform of section 127(2), taking account of its specific uses.

3.108 According to the same CPS data, section 127(1) CA 2003 is frequently used to prosecute behaviour in the context of domestic abuse. In a random sample of 28 prosecutions brought under section 127(1), 46% concerned domestic abuse.[196] Another common type of behaviour prosecuted under section 127(1) is threats made to public sector workers and service providers, such as social workers, health care professionals, housing officers, and school staff. Of the random sample of prosecutions, this kind of behaviour constituted 18%.[197]

3.109 Another advantage of the general communications offences is that they are, in one respect, easier to prove than the stalking and harassment offences. They do not require a "course of conduct", a single instance of offending behaviour is enough.

3.110 Not only are they easier to prove, they also cover some types of online abuse that the stalking and harassment offences do not, namely, those types of abuse that take the form of one-off communications.

3.111 Yet, despite these strengths, the general communications offences, in our view, suffer from problems sufficiently serious to necessitate reform.

## PROBLEMS WITH THE GENERAL COMMUNICATIONS OFFENCES

3.112 The problems with the general communications offences can be grouped under five main headings: vagueness and uncertainty; over-criminalisation; under-criminalisation; unsatisfactory targeting and labelling; and overlapping offences. In what follows, we discuss the problems under each of these headings.

### Vagueness and uncertainty

3.113 A problem shared by the section 1 MCA 1988 offence and the section 127 CA 2003 offence is the uncertainty arising from the use of terms like "grossly offensive" and "indecent". These terms are vague and ambiguous. Their use in these offences may – as we noted in Chapter 2 – be in tension with Article 10 of the European Convention on Human Rights ("ECHR"), which requires that all interferences with freedom of expression are clearly prescribed by law; "clearly" being the operative word.

3.114 In the case of section 1 MCA 1988, the problem is compounded because the grossly offensive or indecent nature of the communication is relevant not only to the conduct element of the offence (the sending of a grossly offensive communication to a victim), but also to the mental element (the intention to cause a victim distress or anxiety). The nature of the communication may constitute evidence that one of the defendant's purposes was to cause the victim distress or anxiety. In other words, the prosecution would suggest to the jury that the communication is so grossly offensive that the defendant's purpose must have been to cause its recipient distress. Hence, the

196 13 out of 28 prosecutions.

197 5 out of 28 prosecutions.

problem of vagueness and uncertainty arises in relation to both the conduct and the mental elements of the offence.

3.115 The term "grossly offensive" has attracted particular controversy. In our Scoping Report, we noted widespread criticism from academics, journalists, lawyers, and human rights organisations such as Big Brother Watch and the Open Rights Group, particularly on the basis of concerns about freedom of expression.[198] This criticism is indicative of a need to consider the extent to which criminal provisions couched in vague terms like "grossly offensive" are consistent with freedom of expression, as protected by Article 10 ECHR. Detailed analysis of the requirements of Article 10 in relation to communications offences can be found in Chapter 2. For convenience, we restate some of that analysis here.

3.116 To determine whether a criminal law provision is compatible with Article 10 (freedom of expression), the European Court of Human Rights' ("ECtHR") analysis proceeds in four stages. The ECtHR must determine:

(1) the existence of an interference;

(2) whether the interference was prescribed by law;

(3) whether the interference pursued a legitimate aim; and

(4) whether the interference was necessary in a democratic society.[199]

3.117 In deciding whether a criminal provision formulated using vague terms – such as "grossly offensive" – is compatible with Article 10, the relevant stage of the analysis is (2): whether the interference was prescribed by law. The Grand Chamber has made clear that Article 10 "not only requires that the impugned measure should have a legal basis in domestic law, but also refers to the quality of the law in question, which should be accessible to the person concerned and foreseeable as to its effects".[200] The Court "must ascertain whether [the provision] is sufficiently clear to enable a person to regulate his/her conduct and to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail".[201]

3.118 As we explain in Chapter 2, we have some concerns that the term "grossly offensive" is too vague to meet the requirement under Article 10 that a restriction on freedom of expression must be clearly prescribed by law.

3.119 It is not clear what properties a communication must possess in order be "grossly offensive", and there is no legal definition of the term to provide further guidance. In the Scoping Report, we noted that this indeterminacy can cause problems for both victims and perpetrators, who may not know if a criminal offence has been committed.

---

198 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 5.5.

199 See, among other authorities, *Karácsony v Hungary* App No 42461/13 (Grand Chamber Decision).

200 *Karácsony v Hungary* App No 42461/13 (Grand Chamber Decision) at [123].

201 *Akçam v Turkey* App No 27520/07 at [91]; similarly, *Grigoriades v Greece* (1999) 27 EHRR 464 (App No 24348/94) at [37].

It also gives rise to interpretative challenges for police, prosecutors, judges and juries.[202]

3.120 Our pre-consultation meetings with stakeholders have corroborated this. Victims of online abuse and the organisations who support them tell us that the existing law in this area is confusing, and it is difficult to know whether a communication will be deemed "grossly offensive". We are also conscious of the risk that vagueness in the law may have a "chilling effect" on innocent or protected speech.[203]

3.121 Admittedly, the problems of vagueness and uncertainty arising from terms like "grossly offensive" have arguably been mitigated, at least to a degree, by CPS guidelines – especially the CPS guidelines on the prosecution of cases involving communications sent via social media – and case law.

3.122 In 2013, the CPS *Guidelines on prosecuting cases involving communications sent via social media* were published (and were updated in 2016 and 2018). As we noted in Chapter 2, these CPS guidelines state that prosecutors should *only* proceed with cases under section 1 MCA 1988 or section 127 CA 2003 if the communication is *more than*:

(1) offensive, shocking or disturbing; or

(2) satirical, iconoclastic or rude comment; or

(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".[204]

3.123 Drawing on *DPP v Collins*[205] and *Smith v ADVFN*,[206] the assessment should be made with reference to "contemporary standards … the standards of an open and just multi-racial society", to determine whether the particular message in its particular context is "beyond the pale of what is tolerable in society".[207]

3.124 The CPS guidelines also state that:

---

202 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 2.102.

203 See Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at paras 5.88-5.89, citing *Singhal v Union of India* (2015) Write Petition (Criminal) No 167 of 201 at para 82.

204 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (last revised 21 August 2018), https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (last visited 07 September 2020).

205 [2006] UKHL 40, [2006] 1 WLR 2223.

206 [2008] EWCA Civ 518.

207 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (last revised 21 August 2018) para 28, https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (last visited 07 September 2020).

> 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?[208]

## Over-criminalisation

### Over-criminalisation arising from vagueness

3.125 Apart from the uncertainty engendered by vagueness of the term "grossly offensive", an additional problem is that it may lead to over-criminalisation: a situation in which conduct is criminalised when it ought not to be.[209]

3.126 Whatever else, the standard of "*gross* offensiveness" is surely higher than that of mere "offensiveness". The question is whether the inclusion of the word "gross" places an effective limitation on the range of communications which can be prosecuted. In a statement announcing plans to issue the aforementioned CPS guidelines on social media prosecutions, then-DPP Keir Starmer QC recognised the difficulty in distinguishing between offensiveness and gross offensiveness. He said:

> The distinction [between offensiveness and gross offensiveness] is an important one and not easily made. Context and circumstances are highly relevant and as the European Court of Human Rights observed in the case of *Handyside v UK* (1976), the right to freedom of expression includes the right to say things or express opinions "… that offend, shock or disturb the state or any sector of the population".[210]

3.127 The CPS guidelines described above set out considerations which may assist in distinguishing the merely offensive from the grossly offensive (the latter being subject to prosecution where the former is not).

3.128 While these guidelines offer some clarity, there is reason to doubt that they have been entirely successful. In the Scoping Report we observed that, even after the publication of the guidelines in 2013, a number of controversial prosecutions took place, such as the prosecution of a man who posted two photographs of body bags, one open, one

---

208 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (last revised 21 August 2018), https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (last visited 07 September 2020).

209 See, for example, D Husak, *Overcriminalization: The Limits of the Criminal Law* (2007), in which the term "overcriminalization" is used to mean that there is too much criminal law and too much punishment; "too much" in the sense that it goes beyond the normative constraints set out by Husak in the book. We note that, by the same reasoning, vagueness and uncertainty could also lead to under-criminalisation: a situation in which conduct is not criminalised when it ought to be.

210 K Starmer QC, *DPP's Guidance on Social Media Prosecutions* (20 September 2012), https://www.scl.org/news/2563-dpp-s-guidance-on-social-media-prosecutions (last visited 07 September 2020).

closed, at the site of the Grenfell Tower disaster.[211] We suggested that the difficulty in determining when a communication crosses the threshold from mere offensiveness to gross offensiveness presents a risk of overcriminalisation.[212]

3.129 That being said, since the Scoping Report, new CPS data has been published, showing a decrease in the number of prosecutions under section 127 of the CA 2003: from 2,950 in 2017-18 to 2,594 in 2018-19. More importantly, the number of prosecutions for grossly offensive or indecent communications has seen the most significant decrease: 2,290 reduced to 1,951; a 14.8% decrease. (By contrast, prosecutions for communications purposely causing annoyance, inconvenience or needless anxiety reduced from 660 to 643; a 2.6% decrease).[213] This data is at least consistent with a shift towards a narrower understanding of "gross offensiveness".

3.130 However, this is not, on its own, sufficient to mitigate concerns about the risk of overcriminalisation. This is because it is not satisfactory to have to rely on prosecutorial discretion to limit, in practice, the scope of an offence that is itself over-broad. Indeed, it is not clear that prosecutorial discretion is succeeding in this regard, at least not in all cases.

### Over-criminalisation arising from an absence of harm

3.131 The communications offences present another, perhaps more fundamental, over-criminalisation problem. In our view, the offences are overbroad in that they cover behaviours which do not necessarily cause harm or pose a risk of causing harm.

3.132 As the Law Commission has written elsewhere, to be deserving of criminalisation conduct should, at minimum, be both harmful and morally wrong. In addition, the perpetrator should have at least a degree of culpability. Harmfulness refers to the degree to which a criminal act causes, or risks causing, harm to others (or, on some views, to oneself). Moral wrongfulness refers to the violation of a moral norm or set of norms. Culpability refers to a degree of fault or blameworthiness on the part of the perpetrator.[214]

3.133 Some communications are both offensive and harmful. The fact that a given communication is harmful, or has potential for harm, is a legitimate (though not sufficient) reason to criminalise it. However, our view is that expressive behaviour

---

211 J Nevett, *Bloke 'who posted Grenfell fire victim pic to Facebook' charged with criminal offence* (16 June 2017), https://www.dailystar.co.uk/news/latest-news/622764/man-arrested-grenfell-fire-victimpicture-facebook-criminal-offence (last visited 07 September 2020); 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), http://www.dailymail.co.uk/news/article-4611862/Man-jailed-posting-Grenfell-Tower-victim-picture.html (last visited 07 September 2020); and S Jones, *Facebook ghoul who photographed dead Grenfell Tower fire victim in body bag is jailed for three months* (16 June 2017), https://www.mirror.co.uk/news/uk-news/facebook-ghoul-whophotographed-dead-10635450 (last visited 07 September 2020).

212 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 5.84.

213 Crown Prosecution Service, *Annual Violence Against Women and Girls Report 2018-19*, at A53, https://www.cps.gov.uk/sites/default/files/documents/publications/cps-vawg-report-2019.pdf (last visited 07 September 2020).

214 See, for example, Reforming Misconduct in Public Office (2016) Law Commission Consultation Paper No 229, at paras 3.5-3.8.

should not be criminalised on the grounds of its offensiveness. This is consistent with views frequently expressed by a range of stakeholders during pre-consultation meetings we held prior to publishing this Consultation Paper, and with the published views of academics such as Bakalis.[215] It is also consistent with the harm principle.

3.134 The harm principle was formulated by John Stuart Mill as a limit on coercive interference with conduct. According to Mill, coercive interference with any form of conduct (and, therefore, any form of expression) can be justified only if the conduct in question causes or threatens harm to others, and interference with the conduct will yield a better balance of benefits over costs than non-interference.[216]

3.135 In his chapter, *Criminalizing Expression: Hate Speech and Obscenity*,[217] L W Sumner applies the harm principle specifically to expression. According to the harm principle, expression cannot be criminalised unless two conditions are satisfied:

(1) the expression causes or poses a risk of harm to others; and

(2) criminalisation will, on balance, be beneficial (taking account of the harms that criminalisation causes, as well as prevents).[218]

3.136 In our provisional view, offensive and even grossly offensive communications do not necessarily meet the first condition: they do not always constitute forms of expression that cause or pose a risk of harm to others. The Oxford English Dictionary includes within its broad definition of "offensive": offending moral sensibilities; causing displeasure; and causing disgust. These effects, even if they are so extreme that they could be described as "gross", are not necessarily harmful.[219] Therefore, even if the term "grossly offensive" could – by way of statutory guidance or statutory definition – be rid of the problem of vagueness, the fundamental problem that it does not track harm, or potential for harm, would remain.

3.137 It is not only the use of the term "grossly offensive" that fails to track harm, thereby giving rise to a problem of over-criminalisation. Two other examples are illustrative of the over-criminalisation problems suffered by section 127 CA 2003:

(1) Since it covers all "indecent" communications sent over a public communications network, the offence covers some private, intimate

---

215 C Bakalis, "Rethinking cyberhate laws" (2018) 27(1) *Information & Communications Technology Law* 86.

216 J S Mill, *Utilitarianism, Liberty, and Representative Government* (1910).

217 L W Sumner, "Criminalizing Expression: Hate Speech and Obscenity" in J Deigh and D Dolinko, *The Oxford Handbook of Philosophy of Criminal Law* (2011).

218 L W Sumner, "Criminalizing Expression: Hate Speech and Obscenity" in J Deigh and D Dolinko, *The Oxford Handbook of Philosophy of Criminal Law* (2011), at p 20.

219 Joel Feinberg has written at length on the distinction between offence and harm: they are distinct concepts and, while "We may (at most) be inclined to rank extreme offenses as greater wrongs to their victims than trifling harms, […] perhaps that is because they may become so offensive as to be actually harmful." J Feinberg, The Moral Limits of the Criminal Law: Volume 2: Offense to Others (1988), at p 3.

communications between consenting adults, such as "sexting".[220] Such communications are not (or certainly not always) not harmful.

(2) Since the offence is complete at the point of the message (or other matter) being sent, it covers the act of uploading documents or images to an online storage facility. But, given that the stored material is unlikely to be seen by anyone other than the sender, it is not clear that this has the potential to lead to any harm.

3.138 Here again, certain elements of the offence mean that it covers conduct which is not necessarily harmful. Regarding the first example, "indecent" communications, much like "offensive" communications, may or may not be harmful. When they are sent between two consenting adults, then, all things being equal, they are not. Regarding the second example, communications "sent" only to one's own secure storage facility are not likely to cause any harm.

3.139 In short, the categories of communication covered by section 1 MCA 1988 and section 127 CA are not, in our provisional view, the type of thing we necessarily ought to criminalise and should not, therefore, be the touchstones of a criminal offence.

### Under-criminalisation

3.140 As we explain above, section 1 MCA 1988 and section 127 CA 2003 contain the broadest and most flexible offences. But even these broad offences are limited in some respects.

3.141 It will be recalled that our overarching criticism of the general communications offences is that the various proscribed characteristics do not map neatly onto the potential for harm. Just as offensive speech may encompass acts both harmful and not, not all harmful speech is appropriately described as grossly offensive or indecent and so on.[221] Therefore, while in some contexts use of the terms like "grossly offensive" and "indecent" present a risk of over-criminalisation, in other contexts, their use may result in under-criminalisation.

3.142 The other main limitation of the section 1 MCA 1988 offence is that the communication must have an intended recipient. This means that some forms of potentially harmful online communication will not be caught. These include, for example, communications

---

220 In the Scoping Report (Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381 at para 6.87) we cited Alisdair Gillespie in support of this view: "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." See A Gillespie, "Obscene conversations, the internet and the criminal law" [2014] *Criminal Law Review* 350, 359. However, it is arguable that this interpretation of "indecent" is too broad, and that the term should be understood more narrowly. We are considering this issue in our project on the taking, making and sharing of intimate images without consent.

221 For the purposes of illustrating the under-criminalisation problem suffered by the general communications offences, it is important to have in mind the various types of abusive online communications. We give a detailed account of behaviours and harms that constitute abusive online communications in Chapters 4 and 6. Here, we simply note some types of communication that, in our view, may not adequately be addressed by the existing criminal law.

posted in a public forum, such as the comments section below an online newspaper article, or posts on a publicly accessible social media page.

3.143 Section 127 CA 2003 does not suffer from these particular problems. But there are contexts in which it under-criminalises. The main problem is the requirement that the message be sent over a public network. This means that messages sent via a private network – such as Bluetooth or a local intranet – are not covered.

3.144 As a result of such limitations, there are some types of online phenomena which are prevalent and have great potential for harm, but which the general communications offences seem unable adequately to address. In what follows, we give some examples.

### Pile-on harassment

3.145 As we noted in the Scoping Report, one such phenomenon arising specifically in an online context is “pile-on” harassment. We recommended that pile-on harassment should be specifically considered in this second phase of the project.

3.146 To reiterate, pile-on harassment is a form of group harassment in which a number of individuals each send messages that, when taken together, cause alarm or distress – even though, taken individually, no message reaches a criminal threshold. This form of harassment is often, though not always, targeted at high profile individuals and can have a devastating impact.

3.147 As we explain above, pile-on harassment may take one of two forms: the harassment may be coordinated or uncoordinated. The coordinated form of pile-on harassment is, at least in principle, criminalised under the PHA 1997. However, the uncoordinated form is not.

3.148 It may be that many individual messages constituting an uncoordinated pile-on will, by themselves, meet a criminal threshold, either under section 1 MCA 1988 or section 127 CA 2003. For example, the set of messages received by Jess Phillips MP included some which were clearly grossly offensive, as well as some which were less clearly so. Some of these messages took the form of “negative rape threats” along the lines of “I wouldn’t even rape you”. While such comments are clearly offensive, and misogynistic, they may not universally be found to cross the threshold into gross offensiveness. One reason for this is that they can be read as a suggestion that this person is not worth committing a crime against.

3.149 It should be noted that genuinely uncoordinated pile-on harassment may occur less frequently than it seems. Research by the Alan Turing Institute found that, sometimes, a pile-on that appears to be organic may actually have been coordinated:

> Another characteristic of raids [a form of pile-on harassment] is their semi-coordinated nature. While a sudden increase in hateful comments to a video is

obvious to an outside observer, what is not obvious is the fact that these comments are part of a coordinated attack. [222]

3.150 For example, the coordination may take place on a relatively obscure "fringe community", such as 4chan, while the abusive content appears on a mainstream site like YouTube.[223]

3.151 Even so, to the extent that genuinely uncoordinated pile-on harassment exists, it is, arguably, under-criminalised by the existing criminal law. It is not covered by the PHA 1997, and many of the communications constituting a pile-on may not be the general communications offences, either. In addition, given difficulties in detecting coordination – especially if it happens in a private forum or on the "dark web" – it may be that a law targeting uncoordinated pile-on harassment would prove useful in tackling covertly coordinated harassment, too.

### Glorification or encouragement of self-harm

3.152 In the Scoping Report, we also recommended that glorification or encouragement of self-harm should be specifically considered in this second phase of the project.

3.153 The existence of online content glorifying, encouraging, or promoting self-harm and suicide has attracted significant media attention and has been linked with the deaths of children and young people. For example, the so-called "Blue Whale Challenge" – an online "suicide game" which sets daily "challenges" for "players" – has been well-documented. Daily "challenges" start with, for example, "wake up in the middle of the night", then escalate to "cut a blue whale into your arm", and finally, to suicide.[224] This is an extreme example of content promoting self-harm. At the more insidious end of the scale are websites and social media pages promoting strict diets that may amount to eating disorders or "orthorexia".[225]

3.154 While encouraging or assisting suicide is a specific offence, criminalised under the Suicide Act 1961, encouraging or assisting self-harm is not. As we note in the Scoping Report, there is an argument that glorifying self-harm may be an inchoate offence.[226] We discuss this in detail in Chapter 6. Here, we simply note that, unless a

---

222 Alan Turing Institute, ""You Know What to Do": Proactive Detection of YouTube Videos Targeted by Coordinated Hate Attacks" (2019), presented at 22nd ACM Conference on Computer-Supported Cooperative Work and Social Computing, https://www.researchgate.net/publication/337134957_You_Know_What_to_Do_Proactive_Detection_of_YouTube_Videos_Targeted_by_Coordinated_Hate_Attacks (last visited 08 September 2020).

223 Alan Turing Institute, ""You Know What to Do": Proactive Detection of YouTube Videos Targeted by Coordinated Hate Attacks" (2019), presented at 22nd ACM Conference on Computer-Supported Cooperative Work and Social Computing, https://www.researchgate.net/publication/337134957_You_Know_What_to_Do_Proactive_Detection_of_YouTube_Videos_Targeted_by_Coordinated_Hate_Attacks (last visited 08 September 2020).

224 See, for example, A Adeane, *Blue Whale: What is the truth behind an online 'suicide challenge'?* (13 January 2019), https://www.bbc.co.uk/news/blogs-trending-46505722 (last visited 07 September 2020).

225 See, for example, S Marsh, *Instagram urged to crack down on eating disorder images* (08 February 2019), https://www.theguardian.com/technology/2019/feb/08/instagram-urged-to-crack-down-on-eating-disorder-images (last visited 07 September 2020).

226 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 12.94.

communication glorifying, encouraging, or promoting self-harm crosses the threshold of "obscene, indecent, or grossly offensive", it cannot be prosecuted under section 127 CA 2003. For similar reasons, it may not be caught by section 1 MCA 1988. It is, therefore, another example of potentially harmful communication that is arguably under-criminalised by the existing law.

### Cyber-flashing

3.155 As well as the types of online communication identified for further consideration in the Scoping Report, there are some additional behaviours that we will specifically consider in this Consultation Paper. Since the Scoping Report was published, there has been a spike in reports of "cyber-flashing": the unsolicited sending of sexual images using digital technology. According to figures from the British Transport Police, in 2019 there were 66 reports of cyber-flashing, compared to 34 reports in 2018, and just 3 reports in 2016.[227] Given the increase in reported incidents of cyber-flashing, it is our view that this type of online communication requires specific consideration.

3.156 A particular form of cyberflashing which has received widespread media coverage is cyber-flashing via Apple's "AirDrop" function to someone nearby. Technological advances may offer greater opportunities for cyber-flashers to target a specific victim without using a public network.[228] And yet, such behaviour is not currently criminal under section 127 CA 2003.

3.157 It is possible that cyber-flashing via AirDrop could be caught by section 1 MCA 1988, since this offence does not include a public network requirement. Indeed, one arrest for cyber-flashing in 2018 was recorded by the British Transport Police as an incident under the MCA 1988.[229] However, if the behaviour is charged under this offence, this means that the prosecution will have to prove that the defendant intended to cause the victim distress or anxiety. This may be difficult since some perpetrators of cyber-flashing may act in the belief that their communication will be welcome (although we know that in a great many cases it is not welcome). Other perpetrators may act for their own sexual gratification – reckless as to whether, but not intending that, the victim will suffer distress or anxiety.[230]

3.158 In summary, there are some types of abusive online communications which ought, arguably, to be criminal but may not be adequately dealt with by the existing criminal law, including the general communications offences. These include:

---

227 See R Speare-Cole, *Spike in unsolicited sexual photos sent over AirDrop on trains, data reveals* (19 February 2020), https://www.standard.co.uk/news/crime/cyberflashing-trains-british-transport-police-a4365886.html (last visited 07 September 2020).

228 See, for example, S Gallagher, *Will Apple iOS 13 Make it Easier for Cyber Flashers to Target Victims?* (24 September 2019), https://www.huffingtonpost.co.uk/entry/will-apple-ios-13-make-it-easier-for-cyber-flashers-to-target-victims_uk_5d8381a0e4b0849d4724c19c (lasted visited 07 September 2020).

229 See R Speare-Cole, *Spike in unsolicited sexual photos sent over AirDrop on trains, data reveals* (20 February 2020), https://www.standard.co.uk/news/crime/cyberflashing-trains-british-transport-police-a4365886.html (last visited 07 September 2020).

230 See, for example, M Sarner, *What makes men send dick pics?* (08 January 2019), https://www.theguardian.com/society/2019/jan/08/what-makes-men-send-dick-pics (last visited 07 September 2020).

(1) uncoordinated group or "pile-on" harassment;

(2) glorification of self-harm; and

(3) cyber-flashing.

### Unsatisfactory targeting and labelling

3.159 We have noted that the section 127 CA 2003 offences both under- and over-criminalise in different contexts. This is related to an additional set of problems, concerning the targeting and labelling of harmful conduct.

#### Public communications network

3.160 One of the main causes of this combination of under- and over-criminalisation is the requirement that the communication takes place using a public communications network. This causes us to question why the substance of the offence lies in the use of a public communications network in the first place.

3.161 It was clear from debates on the Post Office (Amendment) Bill in 1935 (which contained a predecessor offence to section 127 CA) that Parliament's intention was to prevent the public communications networks from being used to abuse members of the public.[231] That being the case, it is an odd formulation. If you are concerned with members of the public receiving menacing messages, say, why criminalise only certain means of delivery? Why would it be one offence to send an indecent message through the postal service or by telegram and another offence to deliver the same letter by hand?

3.162 An alternative explanation is that the offence aims 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 society. This was held by the House of Lords in *Collins*[232] and recently affirmed by the High Court in *Miller.*[233] However, as we observed in our Scoping Report, this justification is ill-suited to the modern context, where most public communications networks – at least of the electronic variety – are not provided and funded by the public for the benefit of the public. Instead, they are created and operated by corporations for profit.[234]

3.163 There is alternative justification for the separate offence. It is true that the administrators of the public communications network are subjected to harm when exposed to these messages. Indeed, we see today the (often severe) psychological harm suffered by employees of social media companies whose job it is to review abusive online communications.

---

231 Hansard (HL), 19 March 1935, vol 96, col 163 to 164.

232 *DPP v Collins* [2006] UKHL 40, [2006] 1 WLR 2223 at [7].

233 *R(Miller) v College of Policing* [2020] EWHC 225 at [269]. Referring to the judgement of the House of Lords in *DPP v Collins,* Mr Justice Julian Knowles said, "It held: (a) that the purpose of s 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 contravened the basic standards of society".

234 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 4.151.

3.164 However, is this – the presence of network administrators – enough on its own to distinguish criminal from non-criminal acts? It seems unlikely. The harm wrought by certain abusive communications clearly extends to victims beyond those employed by the communications network. Privileging the harm suffered by those employees seems difficult to justify.

3.165 Therefore, it seems that one of the core conduct elements of the section 127 offence – the public network requirement – does not reflect any moral blameworthiness on the part of the perpetrator, or at least not any unique moral blameworthiness.

3.166 To a degree, the problem is mitigated by the existence of an alternative offence under section 1 MCA 1988. Some online communications which cannot be prosecuted under section 127 CA 2003 – because they did not use a public communications network – can instead be prosecuted under section 1 MCA 1988, which contains no such requirement.

3.167 However, this position is not entirely satisfactory. Returning to the issue of cyber-flashing, the public network requirement means that, if the perpetrator uses a peer-to-peer messaging service, such as AirDrop, they can only be prosecuted under the MCA 1988, where the mental element is more difficult to prove. If, on the other hand, they use a public communications network, such as SMS, the prosecution need only prove that they intended to send a message of the proscribed character (for example, that they intended to send an indecent message). This seems arbitrary and unfair.

### Grossly offensive, indecent, obscene

3.168 An additional cause of the combination of under- and over-criminalisation is the use of the terms “grossly offensive”, “indecent”, and “obscene”. These terms do not reflect the harmful nature of online abuse, meaning that harmful conduct is not appropriately labelled or targeted: this is bad in and of itself, and also bad from the point of view of guiding behaviour.

3.169 As Bakalis writes:

> Another important issue here relates to identifying the mischief of this offence… the terms ‘grossly offensive’ or ‘indecent’ seem particularly outdated for such a modern problem. It is difficult to see how we can justify criminalising speech on the internet on the basis of ‘gross offensiveness’ or ‘indecency’. When one considers the extent to which the incitement offences under the POA [Public Order Act] have very high thresholds in order to ensure no infringement of the right to freedom of expression, it is difficult to support, without deeper consideration, the existence of such a wide actus reus [conduct element] under the MCA [Malicious Communications Act] which appears to give the state much more power to interfere with online speech.[235]

[235] C Bakalis, “Rethinking cyberhate laws” (2018) 27(1) *Information & Communications Technology Law* 86, at p 99.

## Overlapping offences

3.170 A final problem, which we noted in the Scoping Report,[236] is that the offences under section 127 of the Communications Act 2003 and section 1 of the Malicious Communications Act 1988 sit together somewhat awkwardly, and overlap in ways that cannot readily be explained.

3.171 Originally, section 1 of the MCA 1988 did not apply to electronic communications. When it was amended in 2001 to extend to electronic communications, it appears that the overlap with section 43 of the Telecommunications Act 1984 – the predecessor to section 127 of the CA 2003 – was not adequately considered. The result is that, in some cases, conduct will be covered by both section 127 CA 2003 and section 1 MCA 1988 but, in other cases, only one or other offence could be charged, in a way that seems somewhat arbitrary. One example is cyber-flashing via AirDrop, which is not covered by section 127 CA 2003, but could be covered by section 1 MCA 1988, provided the mental element is met. Another example is the sending of a grossly offensive and publicly accessible Tweet which, lacking a targeted recipient, would likely fall outside the remit of section 1 MCA 1988, but could potentially be prosecuted under section 127(1) CA 2003. [237]

3.172 The fact that the two sets of offences untidily overlap may not, on its own, be a sufficient basis for reform. However, in our provisional view, the other issues we have identified in this Chapter necessitate reform, and the "patchwork" problem could be addressed in the process.

## CONCLUSION

3.173 The breadth of the communications offences under section 127(1) of the Communications Act 2003 and section 1 of the Malicious Communications Act 1988 make them, in one sense, suitable vehicles for addressing online abuse. However, they suffer from sufficiently serious problems to require significant reform. In order to make robust proposals for reform, we need to understand not only the problems with the existing law but also the social problem we are seeking to address. To this end, we devote the next chapter to a discussion of the behaviours constituting online abuse and the harms they cause.

---

[236] Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, Chapter 4 and at para 13.19.

[237] See Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 4.29.

# Chapter 4: Criminalising online abuse: behaviour and harms

## INTRODUCTION

4.1 In Chapter 3, we set out the problems with the existing law. It is not enough, however, to identify problems with the current law and use them as the sole basis for reform. For the purposes of proposing a new offence, it is important to understand the social problem we are seeking to address.

4.2 The Scoping Report was concerned with the existing criminal law relating to abusive and offensive online communications. In this second phase of the project, we continue to be concerned specifically with "communications", rather than other types of harmful online behaviour. However, the proposals in this Consultation Paper are not seeking to address "offensive" communications as such: this is because, as we explain in chapter 3, offensive communications may be, but are not necessarily, harmful.

4.3 In our Scoping Report,[238] we set out the nature of the online environment and the impact of online abuse on victims. This chapter builds on those findings, with the aim of:

- clarifying the nature of online abuse and the types of abusive behaviour that fall within the scope of this Consultation Paper;
- ensuring that no group's experience of online abuse is excluded from our understanding;
- mapping the ways in which abusive online communications give rise to harm; and
- considering how harm could play a role in a new communications offence.

4.4 As part of our research for the Scoping Report we conducted a range of stakeholder events and meetings. In this Consultation Paper, we have drawn on that research. We have held an additional series of meetings with stakeholders, including psychologists and social scientists, as well as victims of online abuse and the organisations who support them. We have also attended workshops, discussion forums, and conferences hosted by external organisations, from which we have learned a great deal.

4.5 We are grateful for the insights of all stakeholders, which have informed and shaped our approach to reform of the law in this area.

---

238 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381.

## ABUSIVE ONLINE COMMUNICATIONS

4.6 The online environment is, as we note in the Scoping Report, hugely complicated.[239] It is also changing rapidly. Since the Scoping Report was published less than two years ago, developments in online communications technology have given rise to new forms of and opportunities for abusive or otherwise harmful content. Examples include: abuse using the so-called "internet of things"; [240] unwanted intrusions into Zoom video calls, otherwise known as "Zoom-bombing";[241] and the controversial phenomenon of "point of view ('POV')" videos simulating domestic abuse and violence on the increasingly popular social media platform, TikTok.[242] This list is by no means complete. These are just a few of the online phenomena to have recently emerged.

4.7 It is worth noting that some harmful developments in the online environment have arisen in the context of COVID-19 social distancing measures, the corresponding surge in internet use,[243] and increased risk of domestic violence.[244] Organisations supporting victims of online abuse have reported a significant increase in the number of people using their services. For example, the Report Harmful Content initiative ("RHC") had more cases in April 2020 than in the entire second quarter of 2019.[245]

---

239 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 2.50.

240 According to researchers at University College London, "internet of things" is "an umbrella term that reflects an evolution of different technologies across a whole spectrum of applications. These range from tiny sensors that collect humidity or temperature levels, to gadgets and household appliances such as "smart" fridges or thermostats, to complex systems such as connected and autonomous vehicles. What makes IoT devices unique is their connectivity. It allows different systems to be interlinked, creating an interdependent network with different devices basically "speaking" to each other." See University College London, *Gender and IoT Research Report, The rise of the Internet of Things and implications for technology-facilitated abuse* (November 2018). For discussion see, for example, J Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity" (2019) 15(1) *St Antony's International Review* 83.

241 K Paul, "Zoom releases security updates in response to 'Zoom-bombings'" (23 April 2020), https://www.theguardian.com/technology/2020/apr/23/zoom-update-security-encryption-bombing (last visited September 2020).

242 See, for example, D Jimenez, *This Disturbing TikTok 'POV' Trend Is All About Domestic Abuse* (02 April 2020), https://www.vice.com/en_uk/article/epg9np/this-disturbing-tiktok-pov-trend-is-all-about-domestic-abuse (last visited September 2020).

243 See, for example, M Beech, *COVID-19 Pushes Up Internet Use 70% And Streaming More Than 12%, First Figures Reveal* (25 March 2020), https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/#114a95a53104 (last visited 09 September 2020).

244 M Townsend, *Revealed: surge in domestic violence during Covid-19 crisis* (12 April 2020), https://www.theguardian.com/society/2020/apr/12/domestic-violence-surges-seven-hundred-per-cent-uk-coronavirus (last visited 09 September 2020).

245 We were told this during the Report Harmful Content Discussion Forum, 13 May 2020.

4.8 In addition, the outbreak of the SARS-CoV-2 pandemic has led to a new wave of online hostility against East Asian minorities[246] and also against Jewish people[247] (we discuss this in more detail below).

4.9 This is an important reminder that the online and offline worlds cannot neatly be separated. Developments in the online environment are influenced by offline events and vice versa. Young people, in particular, tend not to perceive a boundary between the "online" and "offline" aspects of life. This has been a consistent message from stakeholders.[248] Moreover, online and offline abuse are often comorbid.[249] For example, many of the cases of the online harm reported to RHC in April 2020 also had an offline component, such as offline stalking or domestic violence.[250]

4.10 That being said, some forms of harmful communication are particularly prevalent in the online environment, because they are facilitated by online communications technologies or because they are fostered by the characteristics and cultural norms of the internet.[251] For example, the internet of things has facilitated new forms of control and coercion. A "smart" doorbell might allow an abuser to track movements in and out of the house. A thermostat or lighting system can be adjusted remotely in order to "gaslight"[252] a victim.

4.11 To give another example, while "pile-on" harassment[253] does not take place exclusively online (an offline equivalent is, perhaps, severe heckling in a public lecture theatre), the internet makes piling on easier in practical terms: it is easier to find like-minded people with whom to engage in abusive behaviour, and easier to identify, locate, and target victims. From a psychological point of view, such behaviour is encouraged by the disinhibition effect of the internet and by the sense of anonymity online.[254]

---

246 See, for example, B Vidgen and others, *Detecting East Asian Prejudice on Social Media* (08 May 2020), https://arxiv.org/abs/2005.03909 (last visited 09 September 2020).

247 Community Security Trust, *Antisemitic incidents Report* (2019), available at https://cst.org.uk/data/file/9/0/IncidentsReport2019.1580815723.pdf (last visited 09 September 2020), at p 4.

248 This has been the message from stakeholders including Dr Carrie Myers, Holly Powell-Jones (PhD researcher), and Sue Jones (Deputy CEO of Ditch the Label).

249 See, for example, (2018) Law Com No 381, para 1.53, citing APPG on Domestic Violence, *Tackling domestic abuse in a digital age* (February 2017), https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/04/APPGReport2017-270217.pdf (last visited 09 September 2020)

250 We were told this during the Report Harmful Content Discussion Forum, 13 May 2020.

251 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at paras 2.155-2.161.

252 "Gaslighting" refers to tactics of control designed to make a victim doubt their own sanity. See, for example, J Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity" (2019) 15(1) *St Antony's International Review* 83, at p 89.

253 By this we mean uncoordinated group harassment. For a full discussion of pile-on harassment, see Chapter 6.

254 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at paras 8.198-8.199.

4.12 Findings from recent studies give a sense of both the scale and the varieties of online harm:

(1) In a 2019 report commissioned by Ofcom, Jigsaw Research found that 61% of the 2,057 surveyed adults[255] had at least one potentially harmful experience online in the last 12 months.[256] Forty-seven per cent had experienced potentially harmful content or interactions with others, and 29% per cent had experienced something they rated as "harmful" (annoying, upsetting, or frustrating).[257]

(2) In a 2019 report, the NSPCC found that 31% of the 2,004 children[258] they surveyed had seen worrying or nasty online content, and 19% of surveyed secondary school students had seen content which encouraged people to hurt themselves.[259]

(3) According to data collected by National Policing Advisor for Hate Crime, Paul Giannasi, and the National Online Hate Crime Hub, the young climate change activist, Greta Thunberg, is subject to, on average, 151 hateful posts per minute worldwide. When she met with former US President, Barack Obama, this rose to over 500 posts per minute.[260]

4.13 The enormous scale of harmful online communications is an important impetus for reform in this area and a reason for giving special consideration to this mode of communication.[261] Indeed, in the Scoping Report, one of the reasons we gave for

---

255 Aged 16 or over.

256 That is, 61% of respondents selected at least one of the things listed when asked "Which if any of these things have you come across on the internet in the last 12 months?". The things listed were potential online harms, divided into three categories: (1) data; (2) hacking/security; and (3) content/contact with others.

Under (3), content/contact with others, the following things were listed: (i) fake news; (ii) offensive language; (iii) violent\ disturbing content; (iv) unwelcome friend\follow requests/unwelcome contact or messages from strangers; (v) offensive videos/pictures; (vi) harmful/misleading advertising; (vii) hate speech/inciting violence; (viii) bullying, abusive behaviour or threats; (ix) trolling (a person who deliberately says something controversial); (x) people pretending to be another person; (xi) sexual\pornographic content; (xii) spending too much time online; (xiii) encouraging self-harm e.g. cutting, anorexia, suicide; (xiv) encouraging terrorism\ radicalisation; (xv) cyberstalking (harassment from other internet users); (xvi) material showing child sexual abuse.

257 Jigsaw Research, *Internet users' experience of harm online: summary of survey research* (Ofcom 2019), https://www.ofcom.org.uk/__data/assets/pdf_file/0028/149068/online-harms-chart-pack.pdf (last visited 02 December 2019).

258 Aged 12 to 15.

259 H Bentley and others, *How safe are our children? 2019: an overview of data on child abuse online* (NSPCC 2019), https://learning.nspcc.org.uk/media/1747/how-safe-are-our-children-2019.pdf (last visited 29 November 2019), at p 10.

260 This figure comes from internal data generated by the National Online Hate Crime Hub, provided to us by Paul Giannasi.

261 That being said, we are, as the Law Commission has commented elsewhere, reluctant to recommend criminal offences "the commission of which could never be adequately policed". See (2018) Law Com No 381, para2.162, citing Poison Pen Letters (1985) Law Com No 147, para 3.6. We discuss this issue further in Chapter 5.

focussing on online, rather than offline, abuse was that online abuse is a newer and growing phenomenon. In addition, victims of online abuse endorsed this approach and felt that online abuse had not been properly addressed or understood in the same way as offline abuse.[262]

4.14 There is, therefore, good justification for considering harmful online communications as a discrete social phenomenon, as distinct from offline communications. That is the approach we take in this chapter.[263]

### Defining online abuse

4.15 As we state in the introduction to this chapter, the proposals in this Consultation Paper are not seeking to address "offensive" communications as such: this is because, as we explain in Chapter 3, offensive communications may be, but are not necessarily, harmful.

4.16 "Abusive" may be a more apt shorthand for the types of harmful online communications we are seeking to address. However, the identification of certain online communications as abusive is no straightforward matter. Of this difficulty, the Alan Turing Institute has said:

> A challenge for all researchers in the field of online abuse is how it should be defined and what actually constitutes abuse... Part of the problem is that defining online abuse is not a purely scholastic endeavour: just by labelling content as 'abusive' we potentially create a moral and social impetus to constrain and challenge its dissemination online[264]

4.17 Indeed, in a recent workshop hosted by the Alan Turing Institute, and attended by representatives from civil society, policy making bodies, and academics, defining online abuse was identified as a key challenge and priority for future research agendas. Elsewhere, the Alan Turing Institute has written:

> The categorization of abusive content refers to the criteria, and process, by which content is identified as abusive and, secondly, what type of abusive content it is identified as. This is a social and theoretical task: there is no objectively 'correct' definition or single set of pre-established criteria which can be applied. The determination of whether something is abusive is also irreducible to legal definitions as these are usually minimalistic (HM Government, 2019). Similarly, using the host platforms' guidelines is often inappropriate as they are typically reactive and vague. More generally, academia should not just accept how platforms frame and define issues as this might be influenced by their commercial interests.[265]

---

262 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at paras 3.9-3.10.

263 Albeit that, as we explain in Chapter 5, our proposed new communications offence would not apply exclusively online.

264 B Vidgen and others, *How much online abuse is there?* (Alan Turing Institute 2019), https://www.turing.ac.uk/news/how-much-online-abuse-there (last visited 09 September 2020), at p 10.

265 Alan Turing Institute, *Challenges and frontiers in abusive content detection* (01 August 2019), Proceedings of the Third Workshop on Abusive Language Online, pp 80–93, at p 80.

4.18 For the purposes of understanding the social phenomenon we are seeking to address, we agree that we cannot rely on pre-existing legal definitions. Any new offence that we propose should be informed by social reality; we should not limit our understanding of that reality by reference to pre-existing legal definitions. However, in the social sciences, the concept of abuse as it relates to communications is not well-defined.

4.19 In light of the difficulties of articulating something more precise, in the Scoping Report we took a broad view of the concept of "abusive" communication. We noted that, in the Oxford English Dictionary, "abusive" is defined variously as, first, treating someone with cruelty or violence, especially regularly or repeatedly, or secondly, speaking to someone in an insulting or offensive way.

4.20 While these dictionary definitions of abusiveness are a useful starting point, one problem, at least for our purposes, is that they rely, in part, on offensiveness. Especially given the problems with using offensiveness as a touchstone for criminality (set out in Chapter 3), defining abusiveness in terms of offensiveness may lead to unhelpful conceptual confusion.

4.21 The Alan Turing Institute has identified some common themes across different concepts of online abuse. These include the intention of the speaker and the effect of abuse. However, they express scepticism about, in particular, definitions of abuse that rely on its harmful effects. This is, in part, because such definitions "pre-empt the effects" of abuse and may therefore generate circularity.[266]

4.22 They make some progress by noting that existing research tends to divide online abuse into two categories – individual-directed abuse and group-directed abuse – and offer examples of each type of abuse:

> Abuse directed against individuals includes statements such as 'I hate you' or '@USERNAME you tw*t' and group-directed abuse includes statements such as 'Anyone wearing a hijab better watch out or else I'm going to stab them' or 'I want to kill all refugees'.[267] [268]

4.23 This indicates an alternative approach for identifying the social phenomenon to which the term "online abuse" refers, namely, to consider the concrete behaviours that tend to be labelled as such. Powell and others have defined "digital harassment and abuse" in this way:

> digital harassment and abuse is an umbrella term referring to a range of harmful interpersonal behaviours experienced via a range of online platforms, as well as via

---

266 Alan Turing Institute, *Challenges and frontiers in abusive content detection* (01 August 2019), Proceedings of the Third Workshop on Abusive Language Online, pp 80–93.

267 B Vidgen and others, *How much online abuse is there?* (Alan Turing Institute 2019), https://www.turing.ac.uk/news/how-much-online-abuse-there (last visited September 2020), at p 10.

268 We note that the Alan Turing Institute does, however, recognise that the lines between these two categories of abuse can be blurred.

mobile phone and other electronic communication devices (including tablets and online gaming consoles).[269]

4.24 Galop in their Online Hate Crime Report 2020 listed the following as "types of online abuse": insults; threats of physical violence; threats of sexual violence; death threats; doxing;[270] outing;[271] threats to destroy property; and blackmail.[272] This list appears in the context of a survey regarding online abuse as experienced by LGBT+ people and thus reflects the particular types of abuse that LGBT+ people tend to receive. As we explain below, it is important to realise that different groups have different experiences of online abuse. The list is replicated here to give a sense of some of the types of behaviours constituting online abuse; it is by no means complete (nor do we attribute to Galop the intention that it should be taken as complete).

4.25 Notably, however, similar types of behaviour appear in a joint statement by the United Nations Special Rapporteurs on Violence Against Women and Freedom of Expression on gender-based abuse online. These behaviours included: blackmail; threats of sexual assault; sexist comment; intimidation; stalking; surveillance; and dissemination of private content without consent.[273]

4.26 PEN America's Online Harassment Field Manual uses the term "online abuse" interchangeably with "online harassment" and defines these terms according to behaviours they encompass.[274] According to PEN America, such behaviours include but are not limited to: "cyberbullying"; "cyber mob-attacks"; "cyberstalking"; "denial of service attacks"; "doxing"; "hacking"; "hateful speech and online threats"; "message bombing"; "non-consensual intimate images and videos"; "online impersonation"; "online sexual harassment"; "trolling"; and "swatting".[275]

4.27 Commonalities across such lists suggest that, although there is no clearly defined concept of "online abuse", the term is used to refer to a fairly consistent set of

---

269 A Powell and others, "Digital harassment and abuse: Experiences of sexuality and gender minority adults" (2020) 17(2) *European Journal of Criminology* 199 at 201.

270 "Doxing" means the publishing of private or identifying information about a particular individual without their consent. See, for example, L Hubbard, *Online Hate Crime Report* (Galop 2020), http://www.galop.org.uk/online-hate-crime-report-2020/ (last visited 09 September 2020), at p 7.

271 "Outing" is a specific form of "doxing", where the disclosure of information involves linking the identity of someone who is, for example, open about their gender history, sexual orientation, or HIV status to a different context in which they are not. See, for example, L Hubbard, *Online Hate Crime Report* (Galop 2020), http://www.galop.org.uk/online-hate-crime-report-2020/ (last visited 09 September 2020), at p 7.

272 L Hubbard, *Online Hate Crime Report* (Galop 2020), http://www.galop.org.uk/online-hate-crime-report-2020/ (last visited 09 September 2020).

273 See Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 1.50.

274 PEN America, *Online Harassment Field Manual*, https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/ (last visited 01 June 2020).

275 "Swatting" is a practice whereby a hoax call is placed to the police, detailing a false but plausible claim in relation to the victim. The practice takes its name from heavily armed "SWAT teams", who the perpetrator intends should respond to the call, with negative consequences for the victim. See, for example, PEN America, *Online Harassment Field Manual*, https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/ (last visited 01 June 2020).

behaviours. For our purposes, we consider that such behaviours offer the most useful indication of what is meant by "online abuse".

4.28 For the purposes of this Consultation Paper, we adopt the following working definition of "online abuse". Online abuse includes but is not limited to: online harassment and stalking; harmful one-off communications, including threats; discriminatory or hateful communications, including misogynistic communications;[276] doxing and outing; impersonation.

### Types of online abuse within the scope of this Consultation Paper

4.29 On any plausible definition of "online abuse", the term covers some behaviours that are not strictly within the scope of this Consultation Paper. As we explain in the introduction, we are looking in this Consultation Paper at a narrower range of offences and behaviours than those we considered in the Scoping Report. Out of the Scoping Report arose three separate, but connected, projects. Alongside this project, the Law Commission is also undertaking a project addressing hate crime and a project addressing the taking, making and sharing of intimate images without consent. Some of the offences and behaviours considered in the Scoping Report are the specific focus of those other projects and are not the immediate concern of this Consultation Paper. Such behaviour includes "revenge porn", other forms of image-based abuse, and stirring-up hatred.

4.30 This Consultation Paper is specifically concerned with reform of the existing communications offences: section 127 of the Communications Act 2003 and section 1 of the Malicious Communications Act 1988. We are broadly concerned with the types of conduct that are or could be prosecuted under these offences – with the important caveat that, as we explain in Chapter 3, these offences, in our view, both under- and over-criminalise in different respects. We are also specifically concerned with the following:

(1) cyber-flashing, including via AirDrop or other peer-to-peer communications networks;

(2) uncoordinated group harassment, otherwise known as "pile-on" harassment; and

(3) communications "glorifying" or encouraging self-harm; and

(4) "glorification" of violent crime.

4.31 We are conscious that different types of online abuse may not give rise to the same type(s) or degree of harm, through the same causal mechanisms. When we are

[276] Whether or not such communications meet the requirements to be classified as a hate crime under the existing law. We note that the term "online hate" can refer not only to hate crimes that take place online, but more broadly to hateful or otherwise discriminatory online communications. In the glossary, we define "online hate" as follows: "By "online hate" we mean a hostile online communication that targets someone on the basis of an aspect of their identity (including but not limited to protected characteristics). Such communications will not necessarily amount to a hate crime. We note that the College of Policing's Hate Crime Operational Guidance (2014), stipulates that police should record "hate incidents" using a perception-based approach. Again, such incidents may not amount to a hate crime."

considering the harm arising from abusive online communications, we must, therefore, have in mind the specific behaviours we are seeking to address.

4.32 That being said, we have been presented with evidence from stakeholders that many forms of online abuse occur concurrently. For example, RHC's *Pilot Year Evaluation* (2020) stated that:

> It was rare for a client to report just one online 'harm', harms frequently overlapped and intersected with other issues, both on and offline.[277]

4.33 RHC found that various types of online abuse occur in "clusters". For example, according to their report, impersonation, bullying and harassment, and privacy violation form one "cluster"; 20% of RHC cases contained all three of these issues and 44% contained two out of the three (in various combinations). Helpfully, the report provides a qualitative analysis of the relationship between these different types of abuse:

> The way these three issues intersected was largely through someone creating a fake social media profile, masquerading as the client by using their videos, images and other personal data. This profile was used over a period of time to bully the client, by spreading lies about them, 'outing' them or harassing them with abusive language and/or humiliating images and videos.[278]

4.34 To give another example, we have been told that that image-based sexual abuse is often part of a wider course of harassing conduct.[279] These examples suggest to us that, in some cases, it will be artificial to try to isolate the harmful impact of one particular form of online abuse.

4.35 In additional, emerging forms of tech abuse, such as abuse using the internet of things, may involve behaviours that do not fit neatly into a single category of conduct. Some instances of abuse via the internet of things may constitute a communications offence; some may constitute stalking or harassment; and some – depending on the nature of the relationship between the perpetrator and the victim – may be caught by the offence of controlling or coercive behaviour in an intimate or family relationship under section 76 of the Serious Crime Act 2015.

4.36 Finally, some types of abuse, such as coordinated and uncoordinated group harassment, are likely to be experienced in a similar way by a victim, such that findings from research about the impact of the former can, to some extent, be applied to the latter.

---

277 Report Harmful Content, *Pilot Year Evaluation* (2020), https://d1afx9quaogywf.cloudfront.net/sites/default/files/RHC%20Report%20Final%20with%20Logos_0.pdf (last visited 09 September 2020), at p 21.

278 Report Harmful Content, *Pilot Year Evaluation* (2020), https://d1afx9quaogywf.cloudfront.net/sites/default/files/RHC%20Report%20Final%20with%20Logos_0.pdf (last visited 09 September 2020), at p 21.

279 Dr Emma Short reported this to us in a pre-consultation meeting. It is a finding from the as yet unpublished results of the "Harassment and Revenge Porn Survey".

4.37 In light of these considerations, this chapter will consider harms arising from various forms of online abuse, some of which may not fall squarely within the Terms of Reference upon which this Consultation Paper is based.

## ONLINE ABUSE AS EXPERIENCED BY DIFFERENT GROUPS

4.38 In the Scoping Report, we referred to research commissioned by the Guardian into the 70 million comments that had been left on news articles on its site in the previous decade. The findings of that research bear repeating here:

> 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.[280]

4.39 Our pre-consultation meetings with stakeholders have confirmed that different groups have different experiences of online abuse. Experiences of abuse differ in terms of:

- scale;
- type;
- perceptions; and
- impact.

4.40 In the next section, we discuss in detail the harmful impacts of online abuse. However, before doing so, we consider how online abuse is experienced by the following groups: women; LGBT+ people; disabled people; religious groups; and BAME people. Finally, we consider the experience of children and young people.

4.41 We recognise that anyone could be the target of online abuse. Online abuse is often targeted against celebrities, politicians, and other high-profile figures, even if those individuals do not fall within the aforementioned groups. For example, many Members of Parliament are white, straight, able-bodied men and they may nonetheless be subjected to unusually high levels of online abuse as compared to the average person.[281] Yet, at the same time, we are conscious that certain groups are disproportionately affected by online abuse. The experiences of such groups must be included in our understanding of the social problem we seek to address.

---

280 B Gardiner and others, *The dark side of Guardian Comments* (12 April 2016), https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments (last visited 09 September 2020).

281 See, for example, S Ward and L McLoughlin (2020) "Turds, traitors and tossers: the abuse of UK MPs via Twitter" (2020) 26(1) *The Journal of Legislative Studies* 47.

## Women

4.42 As we explain in the Scoping Report, before starting our work on abusive and offensive online communications, we engaged in a public consultation to ask whether it was a suitable project for us to undertake. During this consultation, one concern repeatedly raised was that women are disproportionately likely to be affected by online abuse.[282]

4.43 In 2017, Amnesty International reported that nearly a quarter (23%) of the women surveyed across eight countries said they had experienced online abuse or harassment at least once, and 41% of these said that these online experiences made them feel that their physical safety was threatened.[283]

4.44 The online abuse received by women is qualitatively distinct. For example, Laura Thompson, a PhD researcher at City, University of London, has found that abuse of women on dating apps displays two misogynistic themes. The first of these themes is the "not hot enough" discourse: many men used appearance-related insults to suggest that those women who had rejected them were "fat" and "ugly" with resulting inferior "value" in the online sexual marketplace. The second theme is the "missing discourse of consent": "pickup lines" used by men often took the form of aggressive sexual invitations, and messages from men to women often escalated to include threats of sexual violence and victim-blaming sentiments.[284]

4.45 The scale and qualitative nature of abuse received by women, especially high-profile women, can combine to produce acutely harmful impacts. In their report, Amnesty International included testimony from Laura Bates, founder of the Everyday Sexism Project and author of the book Everyday Sexism, who said that she received around 200 abusive online messages per day, even before she became high-profile:

> 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 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.[285]

---

282 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 1.48.

283 Amnesty International UK, *Amnesty reveals alarming impact of online abuse against women* (20 November 2017), https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/ (last visited September 2020).

284 L Thompson, "'I can be your Tinder nightmare': Harassment and misogyny in the online sexual marketplace" (2018) 28(1) *Feminism and Psychology* 69.

285 Amnesty International UK, *Amnesty reveals alarming impact of online abuse against women* (20 November 2017), https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/ (last visited September 2020). In our 2015 report on Offences Against the Person, we recommended that the offence of threats to kill under the Offences Against the Person Act 1861 should be extended to cover threats to cause serious injury and threats to rape. See "Reform of Offences Against the Person", Final Report (November 2015) Law Com No 361, paras 8.11-8.12. This reform has not yet been implemented.

### LGBT+ people

4.46 LGBT+ people have a unique experience of online abuse. Regarding the different types of abuse, there is evidence to suggest that LGBT+ people are disproportionately affected by doxing and, more specifically, outing.[286] Doxing refers to retrieving and publishing, often by hacking, a person's personal information. This can include full names, addresses, phone numbers, emails, spouse and children names, and financial details. However, LGBT+ people are particularly affected by a specific form of doxing known as "outing", whereby information about their gender identity or sexuality is revealed against their will, sometimes in conjunction with other, aforementioned types of information.

4.47 Research suggests that experiences of online abuse also differ within the LGBT+ community. A study by Powell and others examined the "lifetime prevalence" of 26 behaviours associated with five subtypes of digital harassment and abuse among "sexuality diverse" and "gender diverse" adults. The study found, for example, that transgender participants were more likely to report having experienced someone threatening to physically harm them, someone harassing them for a sustained period, and someone sharing embarrassing details about them than cisgender participants. In fact, transgender participants were most likely to experience 25 of the 26 behaviours, and were therefore significantly more likely to experience poly-victimisation as compared with cisgender participants. Further, according to Galop's *Online Hate Crime Report* (2020) transgender victims were more likely than their cisgender counterparts to experience self-blame, social isolation, shame, depression, fear, stress, and anxiety. For example, 56% of trans respondents said they experienced depression as a result of online abuse, compared to 34% of cisgender respondents; and 72% of trans respondents said they experienced fear, compared to 54% of cisgender respondents.[287]

### Disabled people

4.48 In May 2019, Leonard Cheshire reported a 33% increase in recorded online hate against disabled people between 2016/17 and 2017/18.[288] Their press release included testimony from Janine Howard, who experienced "online disability hate crime" and was supported by Leonard Cheshire:

> People I don't know take my photograph when I am out and about, they post it on social media for others to comment on.

---

286 L Hubbard, *Online Hate Crime Report* (Galop 2020), http://www.galop.org.uk/online-hate-crime-report-2020/ (last visited 09 September 2020).

287 L Hubbard, *Online Hate Crime Report* (Galop 2020), http://www.galop.org.uk/online-hate-crime-report-2020/ (last visited 09 September 2020).

288 Leonard Cheshire, *Online hate crime* (11 May 2019), https://www.leonardcheshire.org/about-us/press-and-media/press-releases/online-disability-hate-crimes-soar-33 (last visited 09 September 2020).

> The comments are nasty, hurtful and leave me feeling frightened and angry. There is no escaping this online abuse if I want to use social media. It's horrible to know that my family might see this abuse online.[289]

4.49 This testimony is consistent with research conducted by Alhaboby and others, which found that participants linked the online abuse they had experienced to their disability in two main ways. First, for some participants the abuse was, as in the example above, directly related to their disability. One participant said: "the language is disgusting and they refer to my disability."[290] Second, most participants said that their disability aggravated the harmful impacts of the abuse.

4.50 While people across many different groups are driven offline or excluded from online opportunities due to the abuse they receive, this seems to be a particular problem for disabled people. In January 2019, the House of Commons Petitions Committee published a report on online abuse and the experience of disabled people. The scope of their inquiry included investigating the impact of online abuse on disabled people:

> We were told that abuse can drive people offline. It prevents people from taking up opportunities that could improve their heath, such as work or volunteering. We heard that this was a particular problem for people who had suffered abuse or unnecessary investigations due to accusations of benefit fraud. It was common to hear from disabled people who had repeatedly abandoned online profiles due to abuse. One participant at our Newcastle event told us that she was on her 17th Facebook account.[291]

4.51 Moreover, the Petitions Committee report suggests that abuse of disabled people tends to be minimised:

> The matter of fact way in which disabled people described being told to harm or kill themselves was notable. People who were being told to kill themselves were dismissed as not understanding "banter" or taking it too seriously.[292]

4.52 Finally, we note that disabled people are targeted by some unique forms of online abuse. For example, the Epilepsy Society have recorded numerous online attacks against people with epilepsy, using strobe lights and flashing images to induce seizures. In particular, the Epilepsy Society reports that on 13 May 2020 their Twitter account, with its 26,000 followers, was attacked with over 200 posts over the course of 48 hours. The posts including flashing GIFs and violent and pornographic content. Many individual followers were personally targeted via private message or on their

---

289 Leonard Cheshire, *Online hate crime* (11 May 2019), available at https://www.leonardcheshire.org/about-us/press-and-media/press-releases/online-disability-hate-crimes-soar-33 (last visited 09 September 2020).

290 Z Alhaboby and others, '"The language is disgusting and they refer to my disability": the cyberharassment of disabled people' (2016) 31(8) *Disability and Society* 1138.

291 Online Abuse and the Experience of Disabled People, Report of the House of Commons Petitions Committee (2017-19) HC 759.

292 Online Abuse and the Experience of Disabled People, Report of the House of Commons Petitions Committee (2017-19) HC 759.

own Twitter feeds.[293] This form of abuse deliberately exploits the condition of those with epilepsy and is inextricably connected with their disability.

### Religious groups

4.53 TellMAMA records anti-Muslim online incidents in five categories: "abusive behaviour", "anti-Muslim literature", "discrimination", "hate speech", and "threats". Between January and July 2019, 185 incidents were reported to them, 84% of which were verified. In addition, they worked with police forces across the UK to identify a further 91 anti-Muslim online incidents. Of course, these figures represent only those incidents reported to TellMAMA or recorded by the police. The total number of incidents is likely to be much higher. Both sets of data showed a spike in the aftermath of the terror attack committed in Christchurch, New Zealand in 2019.[294]

4.54 Community Security Trust ("CST") has recorded increasing numbers of reports of antisemitism online:

> An increase in reports of online antisemitism, particularly on social media, is the largest single contributor to the record total of incidents in 2019. CST logged 697 instances of online antisemitism in 2019, comprising 39 per cent of the annual total and a rise of 50 per cent from the 466 online incidents reported in 2018 (which was 28 per cent of that year's total).[295]

4.55 They have also observed forms of online abuse specifically related to the COVID-19 pandemic. These include the following:

> One example is the phenomenon of coordinated antisemitic 'zoombombing', whereby racists and trolls invade virtual synagogue services and other meetings that are held on Zoom and other video conferencing sites to spread antisemitic abuse. Another is the explosion of antisemitic conspiracy theories that began to populate social media as soon as news emerged of a dangerous new virus spreading across the world. CST has tracked and recorded antisemitic posts on mainstream sites like Facebook and Twitter, and in more obscure corners of the internet where extremists gather, like 4Chan and Gab, all of which are consumed with the same hateful obsession: that the Jews must be behind this awful new menace, and that this crisis is the latest opportunity to spread their hatred.[296]

---

293 Epilepsy Society, *Zach's Law: protecting people with epilepsy from online harms* (July 2020). See also S Elvin, *Trolls attack boy with epilepsy, 8, by sending him hundreds of flashing images* (29 May 2020), https://metro.co.uk/2020/05/29/trolls-attack-boy-epilepsy-8-sending-hundreds-flashing-images-12777199/ (last visited 09 September 2020).

294 TellMAMA, *The Impact of the Christchurch Terror Attack, Interim Report* (2019), https://www.tellmamauk.org/wp-content/uploads/2020/03/The-Impact-of-the-ChristChurch-Attack-Tell-MAMA-Interim-Report-2019-PP.pdf (last visited 0i September 2020).

295 Community Security Trust, *Antisemitic incidents Report* (2019), https://cst.org.uk/data/file/9/0/IncidentsReport2019.1580815723.pdf (last visited September 2020), at p 4.

296 Community Security Trust, *Coronavirus and The Plague of Antisemitism* (2020) available at https://cst.org.uk/data/file/d/9/Coronavirus%20and%20the%20plague%20of%20antisemitism.1586276450.pdf (last visited September 2020), at p 3.

### BAME people

4.56 Race and ethnicity impact experiences of online abuse. As we explain the Scoping Report, there is research to suggest that online abuse is disproportionately directed at black people and people of colour. For example, Amnesty International reviewed nearly one million Tweets sent in the run up to the 2017 general election, and found that Diane Abbott, a black female MP, received almost half of the abusive Tweets sent to all female MPs in that period. Other black female MPs and Asian female MPs received one third more abusive Tweets than their white female counterparts.[297]

4.57 In an analysis of data from the Oxford Internet Institute's 2019 Oxford Internet Survey, the Alan Turing Institute found that "Black people were most likely to be targeted by, and exposed to, online abuse.[298] More precisely, they found that:

> 7.7% of White respondents had received obscene/ abusive emails, compared with 41.1% of Black respondents. A smaller difference also exists for seeing cruel/hateful content online. 26.6% of White respondents had viewed such content whilst 38.6% of Black respondents had.[299]

4.58 The recent death of George Floyd – a 46-year-old black man who died while being arrested in the US city of Minneapolis, Minnesota when a police officer knelt on his neck[300] – received global coverage in mainstream and social media. We note that black people are disproportionately likely to be affected by the viral sharing of videos depicting brutality and violence against them, sometimes resulting in death. Though there may be valid reasons for sharing such videos – in particular, for the purpose of raising awareness – they can also be traumatising, especially for black people.[301]

4.59 Finally, we note that the outbreak of COVID-19 pandemic raises concerns about the spread of Sinophobia and other forms of East Asian prejudice. The pandemic has seen reports of online, and offline, abuse directed against East Asian people,[302]

---

297 Amnesty International UK, *Black and Asian women MPs abused more online* (2017),https://www.amnesty.org.uk/online-violence-women-mps (last visited 09 September 2020). 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 to better train the tool to learn and recognise what abusive tweets look like. We estimate our results are about 64% accurate".

298 B Vidgen and others, *How much online abuse is there?* (Alan Turing Institute 2019), https://www.turing.ac.uk/news/how-much-online-abuse-there (last visited 09 September 2020), at p 33.

299 B Vidgen and others, *How much online abuse is there?* (Alan Turing Institute 2019), https://www.turing.ac.uk/news/how-much-online-abuse-there (last visited 09 September 2020), at p 34.

300 At the time of writing, Derek Chauvin, a (now former) police officer, has been charged with first-degree murder and second-degree manslaughter in relation to George Fletcher's death; BBC News, *George Floyd death: Ex-officer charged with murder in Minneapolis* (30 May 2020), https://www.bbc.co.uk/news/world-us-canada-52854025 (last visited 09 September 2020).

301 See, for example, L Green, *We shouldn't have to witness George Floyd's killing for it to spark outrage* (29 May 2020), https://www.theguardian.com/commentisfree/2020/may/29/george-floyd-killing-videos-black-deaths (last visited 09 September 2020).

302 See, for example, T Wong, *Sinophobia: How a virus reveals the many ways China is feared* (20 February 2020), https://www.bbc.co.uk/news/world-asia-51456056 (last visited September 2020). For analysis of the problem of online abuse directed against East Asian people in the wake of the COVID-19 pandemic, see B

causing the United Nations High Commissioner for Human Rights to call on UN member states to address this form of discrimination.[303]

### Intersectionality

4.60 We acknowledge that the identities mentioned above can intersect. This will also affect an individual's experience of online abuse. Indeed, the findings of the Guardian-commissioned research quoted at the beginning of this section attest to this: the group of writers who received the most abuse included eight women, four of whom were non-white, two of whom were gay, one of whom was Muslim, and one of whom was Jewish. This group of writers also included two black men, one of whom was gay.

4.61 Glitch – an organisation founded by Seyi Akiwowo working to end online abuse – explains:

> When exploring online abuse it is important to note that those with multi-intersecting identities will experience online abuse differently and in most cases be disproportionately impacted… For instance, recent research by Amnesty International revealed black women are 84% more likely to be mentioned in abusive or problematic tweets than white women.[304]

### Children and young people

4.62 One cross-cutting cohort is children and young people. Naturally, the experience of children and young people will differ according to whether they belong to one of the aforementioned groups, amongst other factors. However, there are some points to be made about the experience of children and young people as a group.

4.63 The Alan Turing Institute found that young people are more likely to experience abuse. Specifically, they found that:

> 41.2% of 18-30 year olds had seen cruel/hateful content online, compared with 7.4% of 76+ year olds. Age also impacted whether respondents had received obscene/abusive emails but the relationship was far weaker, ranging only from 13.1% of 18-30 year olds to 6.77% of 76+ year olds.[305]

4.64 We have heard from some stakeholders that, amongst young people – especially University students – there is a culture of normalisation or dismissiveness about the

---

Vidgen and others, *Detecting East Asian Prejudice on Social Media* (Alan Turing Institute 2020), https://arxiv.org/abs/2005.03909 (last visited 09 September 2020).

303 M Shields. *UN asks world to fight virus-spawned discrimination* (27 February 2020), https://www.reuters.com/article/us-china-health-rights-idUSKCN20L16B (last visited 09 September 2020).

304 Glitch, *Online abuse explained* (Glitch was founded in 2017), https://fixtheglitch.org/online-abuse/ (last visited 09 September 2020).

305 B Vidgen and others, *How much online abuse is there?* (Alan Turing Institute 2019), https://www.turing.ac.uk/news/how-much-online-abuse-there (last visited 09 September 2020), at p 34.

harmful impacts of online abuse, with both perpetrators and victims sometimes using the excuse of 'banter' or 'humour' to diffuse the seriousness of this behaviour.[306]

4.65 However, we also heard that this is consistent with an awareness of a risk of harm: the perpetrator may realise the seriousness of their actions, but attempt to minimise this by using humour as an excuse.[307]

4.66 Moreover, normalisation or dismissiveness can exacerbate the harmful impact of online abuse. It may lead to inappropriate strategies being adopted or recommended – that victims should come off social media, for example. Moreover, it may cause victims to supress their emotional response, potentially contributing to more serious psychological harms later down the line.[308]

## CATEGORIES OF HARM ARISING FROM ABUSIVE ONLINE COMMUNICATIONS

4.67 Having clarified the behaviours that constitute online abuse and considered the different experiences of different groups, in this section we set out the categories of harm arising from online abuse, and the relationships between harms.

4.68 In our Scoping Report, we discussed the nature of the harms that can result from online abuse and found that the types of harm that arise are manifold. These include not only psychological harms flowing from, say, threats and harassment, but also physical harms flowing from incitements to violence or self-harm. In the Scoping Report, we enumerated the following types of harm:

(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.[309]

4.69 All of these categories of harm continue to be relevant in the context of this Consultation Paper and, in our view, provide a compelling justification for the criminalisation of certain abusive online communications.

### Emotional and psychological harms

4.70 In the Scoping Report we referred to a study from the US, which found that the most common reactions to online harassment and abuse were "annoyance" (83%) and "anger" (68%), while 22% of respondent victims were scared. We are, however,

---

306 This was a consistent message from stakeholders including Dr Adrian Scott, Dr Carrie Myers, and Holly Powell-Jones.

307 This point was made in our pre-consultation meeting with Dr Carrie Myers and Holly Powell-Jones.

308 This point was made in our pre-consultation meeting with Dr Adrian Scott.

309 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 3.30.

conscious of the need to approach such statistics with caution. It should be noted, for example, that a study by the UK's National Centre for Cyberstalking Research found that the most common reactions to cyber-harassment were "distress" (94.1%) and "fear" (80.9%).[310]

4.71 The research, then, is mixed as to the most common reaction to online abuse. Not all victims have the same response and may experience different "shades of harm".[311] As we explain above, some studies have found that the impact of online abuse varies between different groups (with, for example, transgender victims being more likely to experience depression and fear).

4.72 That being said, there do seem to be common themes in the emotional and psychological effects of online abuse. RHC deals with clients who have experienced a wide range of abusive or otherwise harmful forms of online conduct, from bullying and harassment to suicide content to unwanted sexual advances. In their Pilot Evaluation Study 2020, they found that 32% of their clients reported "negative mental health impacts". Among that 32%, the most common impacts were distress (70%), anxiety (52%), a decline in social functioning (36%), depression (27%), suicidal ideation (13%), agoraphobia (5%) and post-traumatic stress disorder (4%). Eighteen per cent of clients experiencing negative mental health impacts had sought medical treatment.[312]

4.73 The report found that online abuse can cause new mental health problems as well as exacerbating existing problems. One RHC client, who became suicidal as a result of harassment on social media by a relative, described the impact as follows:

> "I have (already) tried to commit suicide with an overdose but she is still carrying on I don't know what to do anymore other than another overdose."[313]

4.74 Aside from the RHC report, much of the existing research on the impacts of online abuse focusses on cyber-stalking and cyber-harassment, rather than one-off communications. As we explain in Chapter 3, cyber-stalking and cyber-harassment perpetrated by a single individual or coordinated group of individuals are, at least in principle, adequately covered by the Protection from Harassment Act 1997. In our view, however, it is possible to extrapolate from the existing research to draw conclusions about the likely impact of behaviours to be addressed by the proposals in this Consultation Paper. As we noted in the Scoping Report, the impact of pile-on harassment is, in many cases, likely to be very similar to the impact of coordinated forms of group harassment. Often, a victim may not know whether the harassment

---

310 A Brown, C Maple, and E Short, *Cyberstalking in the United Kingdom: an analysis of the ECHO pilot survey* (National Centre for Cyberstalking Research 2011), https://www.beds.ac.uk/media/244385/echo_pilot_final.pdf (last visited 29 November 2019).

311 Scoping Report, at 3.28, quoting C Langos, "Cyberbullying: The Shades of Harm" (2015) 22(1) *Psychiatry, Psychology and Law* 106, at p 110.

312 Report Harmful Content, *Pilot Year Evaluation* (2020), at p 23.

313 Report Harmful Content, *Pilot Year Evaluation* (2020), at p 23.

was coordinated or uncoordinated and, regardless, this factor may not significantly affect their experience.

4.75 As in the case of online abuse more generally, responses to cyber-stalking and cyber-harassment can vary. Again, however, research has found that there are common themes. The emotional and psychological impacts include distress, fear, paranoia, and anger. One study, conducted by Dr Emma Short and others, gathered data by means of an online survey from a self-selected sample of 100 anonymous participants who defined themselves as victims of cyber-stalking.[314] Participants' testimony about the negative consequences of cyber-stalking included the following:

> "My whole life stopped because I was in so much fear!"
>
> "I get paranoyed [sic] very easily and reluctant to trust indirect communications"
>
> "I am not so much scared by this, just really... angry, fear plays little part in it for me"[315]

4.76 Psychological symptoms included panic attacks, flash backs and PTSD. Participants stated:

> "I still have flashbacks and experience anxiety when going to my inbox. My health has not been the same since"
>
> "I became very ill… and now suffer complex PTSD/depression as a result of the harassment and abuse"
>
> "all the trauma and stress suffered from the stalking resulted in me miscarrying our child"[316]

4.77 Laura Thompson[317] has also conducted recent research, in the form of interviews with women who have been subject to harassment on dating apps. The impact of such abuse was described by one interviewee as follows:

> …it's quite invasive because it's on your phone and you're in a place, and you're in your home it's – I remember feeling quite under threat and not really being able to control it… I was actually like really shocked and upset for a while, more so than I thought I would be because I've had like a lot worse. But um, yeah I didn't – I felt like, like intruded upon in – yeah and it's the fact that your phone's always like

---

314 E Short and others, "The Impact of Cyberstalking: The Lived Experience - A Thematic Analysis" (2014) 199 *Studies in Health Technology and Informatics* 133.

315 E Short and others, "The Impact of Cyberstalking: The Lived Experience - A Thematic Analysis" (2014) 199 *Studies in Health Technology and Informatics* 133.

316 E Short and others, "The Impact of Cyberstalking: The Lived Experience - A Thematic Analysis" (2014) 199 *Studies in Health Technology and Informatics* 133.

317 Laura Thompson is a PhD researcher at City, University of London.

buzzing it's interrupting you and you're just like ugh until I just blocked him. So yeah it's quite an intrusion I think. Of your personal space.[318]

4.78 Pile-on harassment is likely to have a similar impact. In fact, as we noted in the Scoping Report, harassment committed by a group can have a level of "persistence and escalation" that would be difficult for a single individual to replicate.[319] Therefore, the sense of invasion and inescapability may be greater. Moreover, we have heard anecdotally that, far from levelling off, the emotional and psychological toll of a pile-on increases with each message. It has been described to us by analogy with "Chinese water torture", whereby a person is restrained and subjected to repetitive drips of water on the forehead: it is the cumulative effect that causes serious harm.

4.79 These examples involve repeated behaviour, either by a single perpetrator or multiple perpetrators. However, we have learned from stakeholders that some forms of one-off online communication can have a similarly serious emotional and psychological impact.

4.80 One such behaviour is cyber-flashing. Broadly, cyber-flashing involves the sending of unsolicited sexual images. We have learned from stakeholders that cyber-flashing can take various forms. Sometimes, cyber-flashing is part of a wider course of harassing conduct that takes place on a dating app. Other times, large quantities of mixed media are "dumped" onto strangers' phones at the same time.

4.81 A particularly well-documented form of cyber-flashing involves a man sending an unsolicited photograph of his genitals to a woman via Apple's "AirDrop" function. In the paradigm case, the perpetrator and victim are strangers and the incident is a one-off.[320] The perpetrator is able to target the victim because of the way that AirDrop works: an iPhone user can locate other iPhones within range and select a recipient according to the name of their iPhone, provided the recipient's AirDrop settings are such that their iPhone is publicly discoverable. The perpetrator can then "share" an image with their chosen recipient. The recipient is free to "decline" the image, but a preview will automatically appear on their screen.

4.82 Former HuffPost journalist and victim of cyber-flashing, Sophie Gallagher, collected testimony from 70 other women who had also been subjected to cyber-flashing.[321] The following are quotations from some of these women, describing the emotional and psychological impact cyber-flashing had on them:

---

318 Laura Thompson provided us with this unpublished research.

319 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 3.78.

320 See, for example, S Gallagher, *Will Apple ios13 make it Easier for Cyberflashers to Target Victims* (24 September 2019), https://www.huffingtonpost.co.uk/entry/will-apple-ios-13-make-it-easier-for-cyber-flashers-to-target-victims_uk_5d8381a0e4b0849d4724c19c (lasted visited 11 November 2019).

321 S Gallagher, *70 Women On What It's Like To Be Sent Unsolicited Dick Pics*, (12 July 2019), https://www.huffingtonpost.co.uk/entry/cyberflashing-70-women-on-what-its-like-to-be-sent-unsolicited-dick-pics_uk_5cd59005e4b0705e47db0195 (last visited 09 September 2020).

"It made me feel really violated. I felt very exposed that I could be sent something in the middle of the day without warning."[322]

"I felt pretty vulnerable for the rest of my trip and it was scary not knowing who it was but that they might be looking at me or potentially follow me off the train."[323]

"The likelihood someone actually wants to receive a dick pic is like 1%. I was mostly shocked and disgusted as well as embarrassed other people might have seen that content on my phone screen."[324]

"I felt frightened, ashamed, confused and just pushed it to the back of my mind. It is only now I realise it's not ok and just hope that man did not go on to hurt someone."[325]

"I felt jittery for the rest of the journey and kept looking at the men seated and standing around me. I thought about it quite a lot for a long time afterwards."[326]

4.83 Refuge – a charity supporting women, children, and men experiencing domestic violence – told us about other types of one-off communication that can cause serious emotional and psychological harm. For example, for a person who has escaped domestic abuse and is now living in a refuge, a message from their abuser saying, "I just saw you in the supermarket" could be "petrifying" and intended to cause immense distress. [327] Here, it is important to note that the message may, on the face of it, seem innocuous. Yet, understood in context, it is seriously harmful.

4.84 Similarly, a one-off incident whereby the perpetrator shares or threatens to share private information (otherwise known as "doxing" or "outing") can – especially in communities where such information is particularly sensitive – cause serious distress, anxiety, and fear.[328]

4.85 To summarise, it seems clear that online abuse is likely to have a negative impact on mental health. Some common impacts appear to be:

- distress;
- anxiety; and
- paranoia.

4.86 In the more serious cases, online abuse can lead to:

---

322 Jess Shepherd, 28, Manchester, on AirDrop at a restaurant.

323 Chloe Matthbury, 28, Leeds, on AirDrop on a train.

324 Natalie Richardson, 26, Leeds, on Snapchat on a train.

325 Suzy Bennett, 41, Devon, on Facebook Messenger and Twitter.

326 Ella Whiddet, 23, London, on AirDrop on a train.

327 Refuge provided us with this example in a pre-consultation meeting.

328 Again, this example was provided to us by Refuge in a pre-consultation meeting.

- depression;
- post-traumatic stress disorder; and
- suicidal ideation.

4.87 The impact of online abuse is not limited to emotional and psychological harms. For example, one study found that "the ramifications of cyberstalking are widespread, affecting psychological, social, interpersonal, and economic aspects of life."[329] In what follows, we outline these other categories of harm.

### Physiological harms

4.88 As we noted in the Scoping Report, there is research to suggest that online abuse has physiological, as well as psychological, impacts. We referred to a study conducted in the Czech Republic, which found that teachers who had been victims of cyber-attacks and cyber-bullying had experienced physical symptoms including "sleep disorders, headaches, stomach-ache, lack of concentration or reduced immunity".[330]

4.89 We also referred in the Scoping Report to a literature review conducted by the researchers from the Universities of Oxford, Birmingham, and Swansea, which found that young people (aged 25 and under) who were victims of cyberbullying were more than twice as likely to exhibit suicidal behaviour as non-victims.

4.90 More recently, Ditch the Label's Annual Bullying Survey 2019 found that, of those participants who had been bullied within the last 12 months – 74% of whom experienced cyber-bullying – 26% self-harmed, 12% developed an eating disorder, 11% attempted suicide, and 6% abused drugs or alcohol.[331] In the worst cases, online abuse can lead to death.

4.91 We observe that these kinds of physiological impacts seem often to be causally connected to the psychological impacts of abuse. Conditions like sleep disorders or headaches can be regarded as physical symptoms of a psychological condition. Similarly, damaging behaviours like self-harm or disordered eating flow from the psychological impact of the abuse – albeit that a victim may not necessarily be conscious of this at the time. Ditch the Label's report includes the following commentary from Rebecca Barrie, a psychotherapist:

> It may be that while we don't have an immediate emotional reaction to the bullying, psychologically it is impacting by leaving a mark that changes how we behave. For example if we are continually told that we are stupid or ugly or don't belong, we may, in the moment, keep our heads down and not feel an emotion, while simultaneously

---

329 J Worsley and others, "Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses" (2017) 7(2) *Sage Open 1*, at p 1.

330 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 3.37, citing K Kopecky and R Szotkowski, "Cyberbullying, cyber aggression and their impact on the victim – The teacher" (2017) 34 *Telematics and Informatics* 506, at p 515.

331 Ditch the Label, *The Annual Anti Bullying Survey* (2019), https://www.ditchthelabel.org/wp-content/uploads/2020/05/The-Annual-Bullying-Survey-2019-1-2.pdf (last visited 09 September 2020), at p 18.

believing what is being said about us. If we believe what the people bullying have told us about ourselves we can end up making unhealthy decisions.[332]

4.92 We also note that there are some specific forms of online abuse that directly cause physical injury. As we mentioned above, one documented example of such behaviour involves a perpetrator posting a video clip of flashing strobe lights on the social media pages of organisations supporting people with epilepsy, thereby inducing seizures.[333]

### Exclusion from public online spaces and other social and interpersonal harms

4.93 Short and others have found that cyberstalking and harassment can have negative social effects: "damaged reputation, damaged family relations or loss of work either directly or indirectly as a result of the harassment and a damaged reputation".[334] Participants in their study said:

> "[the stalker] impersonated me online sending out emails and status updates that ruined my reputation"
>
> "I have been unable to work properly, as I have felt sullied, damaged, and abused."
>
> "the stalking behaviour caused irrevocable dmage [sic] to family relations"[335]

4.94 We observe that social and interpersonal harms seem often to flow from the initial emotional and psychological harm. For example, one study found that such harms are a result of coping strategies victims feel compelled to adopt: "to adapt, some victims made major changes to both their work and social life, with some ceasing employment and others modifying their usual daily activities."[336]

4.95 In some cases, the relationship between emotional or psychological and interpersonal harms can be symbiotic. Especially for those victims for whom the online space is a key source of social interaction, the impact of online abuse can be a vicious cycle: the emotional and psychological impact leads to withdrawal from online communities which in turn exacerbates emotional and psychological harms. The RHC report includes the following testimony:

---

332 Ditch the Label, *The Annual Anti Bullying Survey* (2019), available at https://www.ditchthelabel.org/wp-content/uploads/2020/05/The-Annual-Bullying-Survey-2019-1-2.pdf, (last visited 09 September 2020), at p 18.

333 Epilepsy Society, *Zach's Law: protecting people with epilepsy from online harms* (July 2020). See also S Elvin, *Trolls attack boy with epilepsy, 8, by sending him hundreds of flashing images* (29 May 2020), https://metro.co.uk/2020/05/29/trolls-attack-boy-epilepsy-8-sending-hundreds-flashing-images-12777199/ (last visited September 2020).

334 E Short and others, "The Impact of Cyberstalking: The Lived Experience - A Thematic Analysis" (2014) 199 *Studies in Health Technology and Informatics* 133.

335 E Short and others, "The Impact of Cyberstalking: The Lived Experience - A Thematic Analysis" (2014) 199 *Studies in Health Technology and Informatics* 133.

336 J Worsley and others, "Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses" (2017) 7(2) *Sage Open 1*, at 1.

> I (was) already on medication for my depression and suicide attempts...I don't go online to be abused. As someone with agoraphobia…it is my only way to interact with friends and the wider world. I can feel this slipping away right now.[337]

### Economic harms

4.96 Related to harms mentioned in the previous subsection – exclusion for online spaces and other social harms – online abuse can also have a negative economic impact. Some of the testimony above indicates that online abuse can affect the ability to work, potentially resulting in a loss of income.

4.97 Further, as we explained in the Scoping Report, online abuse can deprive victims of the "economic opportunities associated with a vibrant online presence".[338] For example, Marshak noted that:

> 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.[339]

4.98 Here again, we observe that at the root of this kind of harm often lies emotional and psychological harm. In some cases, economic harm arises as a result of withdrawal from the online space, which itself can be seen as a coping strategy or response to the initial emotional or psychological impact.

4.99 In other cases, economic harm arises from reduced capacity for work; a consequence of the initial emotional or psychological harm experienced by the victim.

### Wider societal harms

4.100 As we outlined above (as well as in the Scoping Report), different groups have different experiences of online abuse. Experiences differ in terms of scale, type, impact, and perceptions of online abuse.

4.101 Online abuse disproportionately directed towards particular groups can, as we explain in the Scoping Report, cause wider societal harms as well as harm to particular victims. It can contribute to a lack of social cohesion. It can also precipitate the withdrawal of certain groups from public life and public debate; which, arguably, is bad for society as a whole.[340]

---

337 Report Harmful Content, *Pilot Year Evaluation* (2020), at p 23.

338 (2018) Law Com No 381, para 3.45, citing DK Citron, "Cyber Civil Rights" (2009) 89 *Boston University Law Review* 61, at p 62.

339 (2018) Law Com No 381, para 3.46; E Marshak, "Online Harassment: A Legislative Solution" (Summer 2017) 54(2) *Harvard Journal on Legislation* 503, at p 510.

340 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 3.62.

4.102 For example, Glitch records the following societal impacts of online abuse against women and girls:

> Online abuse has a "silencing effect" on all its victims, but particularly on marginalised groups like women and girls. Social media platforms are often critical spaces for individuals to exercise the right to freedom of expression. However, according to Amnesty International, online violence and abuse are a direct threat to this freedom of expression and access to information. Upon suffering online abuse, many women and girls may be forced to abandon their profiles and 76% of women who experienced abuse or harassment on a social media platform changed to the way they use the platforms. Many of them (32%) even stop posting content that expressed their opinion on certain issues.[341]

4.103 In addition:

> Online abuse ends up preventing women and girls from accessing relevant information, expressing their opinions and participating in public debates which in turn negatively impacts on both progress towards gender equality and our democracy.[342]

## MODALITIES OF HARM

4.104 Having set out the categories of harm arising from online abuse, in this section we consider the various "modalities of harm". In other words, we now turn to consider, not the "what", but the "how" of harm arising from online abuse.

4.105 As we explain above, some forms of online abuse can directly cause physical harm. We refer to a documented example of such behaviour where a perpetrator posts a video clip of flashing strobe lights on the social media pages of organisations supporting people with epilepsy. Such communications have caused seizures.[343] A lot of online communications, though, consists of speech of a kind which, it has been thought by some, is not harmful at all. As we said in Chapter 2: this view is captured by the saying "sticks and stones may break my bones but words can never hurt me".

4.106 However, in this chapter and in the Scoping Report, we draw on a considerable body of recent empirical research showing the serious harms that can arise from abusive forms of online speech. This suggests that the view that speech cannot be harmful is outdated and misconceived.

4.107 The empirical research is also supported by a body of theoretical literature arguing that speech is not, or at least not always, simply inert words or ideas. Instead, speech

---

341 Glitch, *Impact of Online Abuse,* (Glitch was founded in 2017), https://fixtheglitch.org/impactofonlineabuse/ (last visited 09 September 2020).

342 Glitch, *Impact of Online Abuse,* (Glitch was founded in 2017), https://fixtheglitch.org/impactofonlineabuse/ (last visited 09 September 2020).

343 C Duncan, *Hackers target people with epilepsy with mass strobe cyberattack designed to trigger seizures, advocacy group warns* (17 December 2019), https://www.independent.co.uk/news/world/americas/hackers-epilepsy-strobe-cyberattack-seizures-videos-kurt-eichenwald-a9249856.html (last visited 09 September 2020).

is often better understood as a kind of act: a "speech act". As we explained in Chapter 2, Rae Langton, drawing on J L Austin's seminal work *How to Do Things with Words*,[344] has argued that hate speech is a kind of speech act; one that does something distinctively harmful to a particular group.[345]

4.108 To recap what we say in Chapter 2: speech acts, according to Langton, may be harmful in a *constitutive* sense and a *causal* sense. In other words, a speech act may be harmful in and of itself (the constitutive sense) or harmful in terms of its effects (the causal sense).[346] The causal harms of speech acts include the emotional and psychological impact on the target, such as distress, anxiety, trauma, and so on. They also include negative impact on social attitudes, such as stirring up hatred or reinforcing widely-held negative stereotypes – whether actual or likely.

4.109 In Chapter 2, we also explained that the harms of expressive behaviour can be further subdivided: causal harms may be *direct* or *indirect*. L W Sumner writes that harm is direct if "it results from exposure to the messages by members of the target group themselves."[347] Direct harms therefore include emotional and psychological harms suffered by the target. Harm is indirect if it "work[s] through the mediation of attitudes and conduct on the part of an audience other than the target groups themselves."[348] Indirect harms therefore include incitement of violence and more diffuse societal harms, such as diminished social cohesion, or reduced representation of certain social groups in positions of power.

4.110 In short, expression can be harmful in a variety of ways or, put another way, there are various modalities of harm. Expression can involve:

(a) constitutive harms;

(b) direct causal harms; and

(c) indirect causal harms – which may be more or less diffuse.

4.111 As we explain in what follows, this taxonomy offers a useful framework for thinking about which harms to include as the basis of a new offence.

### Emotional and psychological harm as the basis of a new offence

4.112 The taxonomy set out above, regarding different modalities of harm, offers a principled justification for making emotional and psychological harm the basis of a new offence. An abusive online communication may involve: constitutive harms; direct causal harms; and indirect causal harms. As we explained in the preceding section, the harms of online abuse can be grouped into five categories: (1) psychological effects

---

344 J L Austin, *How to do things with words* (2nd ed 1962).

345 R Langton, "The Authority of Hate Speech" (2018) 3 *Oxford Studies in Philosophy of Law*.

346 See for example, R Langton, "Hate Speech and the Epistemology of Justice" (2016) 10 *Criminal Law and Philosophy* 865, at 867.

347 L W Sumner, "Criminalizing Expression: Hate Speech and Obscenity" in J Deigh and D Dolinko *The Oxford Handbook of Philosophy of Criminal Law* (2011), at p 24.

348 L W Sumner, "Criminalizing Expression: Hate Speech and Obscenity" in J Deigh and D Dolinko *The Oxford Handbook of Philosophy of Criminal Law* (2011), at p 24.

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. Harms in category (1) – emotional and psychological harms – seem consistently to be direct causal harms of online abuse.

### Direct and indirect harms of online abuse

4.113 In this chapter we set out research by psychologists, social scientists, charities, and NGOs into the harms arising from online abuse. In our view, this research suggests that, in many cases, indirect harms in categories (2), (3), and (4) flow from direct harms in category (1). Emotional and psychological harm are often first in the causal chain of harms. Other harms, such as social, economic, and physiological harms, tend to be the knock-on effect, flowing from the initial emotional and psychological harm.

4.114 In the case of category (4) – economic harm – the chain of causation might work like this: the victim suffers serious emotional distress as a result of abusive online communications sent by perpetrator; this develops into depression and anxiety; as a result of having depression and anxiety, the victim is unable to continue working; the victim then suffers loss of income and or business opportunities.

4.115 In the case of category (2) – physiological harms such as self-harm – the chain of causation might work like this: the victim suffers from depression and body dysmorphia; the victim's psychological symptoms are exacerbated by content glorifying self-harm; as a result, the victim commits an act of self-harm.

4.116 In the case of category (3) – exclusion from online spaces – the chain of causation might work like this: the victim suffers serious emotional distress as a result of the abusive online communications they receive; this causes the victim to leave the online communities of which they were part; the victim then feels isolated and suffers further distress.

4.117 Indirect harms in category (5) are more diffuse and the chain of causation is more difficult to map. As we explain above, the harms might include diminished social cohesion, or reduced representation of certain social groups in positions of power. These harms come about through a complex web of interactions between the attitudes and actions of different actors. The precise role of any given abusive communication may be difficult to map. This is a problem because, as Sumner puts it:

> The case for criminal regulation is weakest where the harms in question (such as the social inequality of visible minorities and women) are widespread and diffuse and the causal link with speech remote and speculative.[349]

4.118 Where this is the case, "it is difficult to justify coercion (especially the extreme form of coercion exemplified by the criminal law) rather than reliance on such less intrusive

---

[349] L W Sumner, "Criminalizing Expression: Hate Speech and Obscenity" in J Deigh and D Dolinko *The Oxford Handbook of Philosophy of Criminal Law* (2011), at p 33.

measures as education, antiracism and antisexism campaigns, counterspeech, and so on."[350]

4.119 However, our provisional view – based on the empirical evidence set out in this chapter – is that many abusive online communications of the kind that contribute to wider societal harms are likely also to cause emotional and psychological harms to the individuals or members of the group towards whom they are directed or who see them. Therefore, an offence based on emotional and psychological harm may nonetheless be effective in addressing such communications, without necessarily making wider societal harm part of the offence itself.[351]

4.120 This kind of argument could also apply in relation to other categories of harm. We accept that the chains of causation mapped out above will not fit every given case of online abuse. Consider, for example, a victim of online stalking who changes her behaviour to avoid offline or online spaces where she knows or suspects the perpetrator will be. This change of behaviour may be motivated by other rational reasons, apart from a desire to avoid emotional distress. If this is the case, harms like social exclusion or loss of economic opportunities that result from the change in behaviour will not be rooted in emotional or psychological harm. And yet, the stalking victim is likely *also* to have suffered emotional distress.

4.121 In short, it seems to us that emotional and psychological harm is the "common denominator" of online abuse. Therefore, a potential new offence would be capable of addressing a wide range of harms flowing from abusive online communications, even if the definition of harm were limited to emotional and psychological harm: the offence would nonetheless cover abusive behaviour that indirectly causes harms in categories (2), (3), (4), and (5).

### Alternative offences to address other direct causal harms

4.122 As we explain in the preceding paragraphs, where it is not true that emotional and psychological harms are first in a causal chain of harms, it may well be the case that they *accompany* other harmful impacts of online abuse.

4.123 One example of online abuse that directly causes physical harm is the deliberate exposure of people with epilepsy to flashing strobe lights. As we stated above, the Epilepsy Society has reported an attack on their Twitter account, with over 200 posts over the course of 48 hours, many of which included flashing images. In such cases, a victim is likely to experience serious emotional distress *in addition* to physical harm in the form of seizure. Hence, a potential criminal offence based on emotional and psychological harm would likely cover this kind of conduct.

4.124 However, where one of the direct harms caused by the communication amounts to physical injury, the conduct will, or should, be caught by a better suited offence. In the

---

350 L W Sumner, "Criminalizing Expression: Hate Speech and Obscenity" in J Deigh and D Dolinko *The Oxford Handbook of Philosophy of Criminal Law* (2011), at p 33.

351 Wider societal harms may be taken into account when deciding whether a characteristic should be protected for the purposes of hate crime legislation. For discussion, see the Law Commission's separate but related Consultation Paper on hate crime, available at www.lawcom.gov.uk.

United States, John Rayne Rivello was charged with criminal cyberstalking with the intent to kill or cause bodily harm after sending Kurt Eichenwald, a journalist who has written extensively about his experiences with epilepsy, a Tweet including flashing strobe lights.[352]

4.125 In England and Wales, communications causing physical harm, including a recognisable psychiatric illness, may be covered by the law on offences against the person. The current law covers, at least in principle, three kinds of communication:

(1) communications directly causing a bodily harm, including recognised psychiatric illness;

(2) communications which are otherwise assaults; and

(3) communications causing a person to take a poison or other destructive or noxious thing.

4.126 Most offences against a person are contained within the Offences Against the Person Act 1861 ("OAPA 1861"). These include (in ascending order of seriousness):

(1) assault, covered by the common law and section 39 OAPA 1861;

(2) assault occasioning actual bodily harm, covered by section 47 OAPA 1861;

(3) maliciously inflicting grievous bodily harm or wounding, covered by section 20 OAPA 1861; and

(4) maliciously causing grievous bodily harm or wounding, with intent to cause grievous bodily harm, covered by section 18 OAPA 1861.

4.127 In addition to more obvious types of physical harm, courts have held that "bodily harm" includes recognisable psychiatric illnesses (though not psychological injury falling short of recognisable psychiatric illness).[353]

4.128 Furthermore, the "infliction" of an injury does not require harm to be applied directly. An assault may be committed by a defendant making a telephone call which causes a victim to fear immediate and unlawful violence.[354]

4.129 This means that a defendant who made a series of silent telephone calls to three victims, causing mental harm to each, could be guilty of assaults occasioning actual bodily harm under section 47 OAPA 1861. A defendant who communicated with a

---

352 C Kang, *A Tweet to Kurt Eichenwald, a Strobe and a Seizure. Now, an Arrest* (17 March 2017), https://www.nytimes.com/2017/03/17/technology/social-media-attack-that-set-off-a-seizure-leads-to-an-arrest.html (last visited 09 September 2020).

353 *R v Ireland* [1998] AC 147; R v Dhaliwal [2006] EWCA Crim 1139, [2006] 2 Cr App R 24.

354 *R v Ireland*, above.

victim by a variety of means, causing the victim a severe depressive illness, could be guilty of maliciously inflicting grievous bodily harm.[355]

4.130 Similarly, then, someone who sends flashing images to a person with epilepsy, thereby causing a seizure, could potentially be guilty of an offence against the person.[356]

4.131 In our provisional view, an offence against the person may, in any case, be a more appropriate way of addressing this kind of behaviour. We are wary of viewing every harmful online act through the lens of communications offences: the internet is essentially a tool or medium, by which or through which many different kinds of act can be committed. We should be open to the possibility that some of these acts may be better understood as, say, an offence against the person or a sexual offence and not, or at least not only, a communications offence.

## CONCLUSION

4.132 The categories of harm arising from online abuse are manifold, and extend far beyond emotional and psychological harms. However, it seems consistently true of abusive online communications that they directly cause, or are likely to cause, emotional or psychological harm to those who see, hear, or otherwise encounter them. There is, therefore, good reason to make emotional and psychological harm the basis of a new communications offence. In Chapter 5, we make proposals for reform on this basis.

---

355 *R v Ireland*, above. The mental harm caused by the first defendant was described in that case as "psychological damage" but the appropriate term has since been clarified as being "psychiatric illness"; *R v Dhaliwal* [2006] EWCA Crim 1139, [2006] 2 Cr App R 24.

356 Further, if there were evidence that the offender was motivated by or demonstrated hostility on the basis of disability, then an aggravated OAPA offence could be charged (for assault, assault occasioning actual bodily harm and maliciously inflicting grievous bodily harm or wounding, but not for the section 18 OAPA offence –maliciously inflicting grievous bodily harm or wounding *with intent* – which does not have an aggravated version). For further discussion of aggravated offences under hate crime legislation, see the Law Commission's separate Consultation Paper on hate crime, available at www.lawcom.gov.uk, in which we propose an aggravated version of section 18 OAPA.

# Chapter 5: The proposed new communications offence

## INTRODUCTION

5.1 Having explained, in Chapters 3 and 4, the problems with the existing law and the social problem we are seeking to address (namely, abusive online communications), in this Chapter we set out our provisional proposals for reform.

5.2 We begin by explaining our approach to reform, including a consideration of the role of the criminal law, an explanation of the forms of communication covered by the proposed new offence, and justifications for adopting a harm-based model.

5.3 Next, we set out the proposed new offence and, for comparison, the offence under section 22 of the New Zealand's Harmful Digital Communications Act 2015, to which some aspects of our proposals are indebted. Given that the New Zealand offence, like our proposed new offence, is a harm-based model, it has been a particularly useful comparator.

5.4 The bulk of the Chapter is devoted to explaining each element of the proposed new offence, and the justifications for the provisional choices we have made.

## OUR APPROACH TO REFORM

5.5 In this section, we explain our approach to reform: the role of the criminal law; the technologically neutral nature of the proposed new offence; and the justifications for adopting a harm-based model.

### The role of the criminal law

5.6 In Chapter 4, we described the behaviours and harms constituting online abuse. In our view, the harms arising from abusive online communications provide a compelling justification for a new criminal offence to address the worst of this behaviour, especially given the problems with the existing law. However, we recognise that the criminal law has a limited role to play and exists within a wider ecosystem of solutions. Other solutions, aside from the criminal law, include:

- regulation and self-regulation of social media platforms;
- digital citizenship solutions, such as counter-speech;
- education.

5.7 The Government's White Paper on Online Harms[357] contains proposals for a liability regime in which platforms will be answerable to a regulator for content hosted on their sites. In any case, these platforms already exercise (or have the ability to exercise) considerable control over content on their sites, by way of "community standards".[358]

5.8 Other important work to tackle abusive or otherwise harmful online communications is being undertaken by stakeholders. For example, the Centre for Countering Digital Hate has produced a practical guide to tackling some forms of online hate, particularly trolling: *Don't Feed the Trolls*.[359] Dr Carrie Myers and Dr Holly Powell-Jones have told us about their work on educating children and young people about the safe and legal use of the internet.

5.9 On the one hand, the enormous scale of online abuse provides an impetus for reform. Equally, though, we are conscious that a criminal offence covering such a high volume of activity would be very difficult to enforce in practice, given the limited resources of the criminal justice system. Solutions outside of the criminal law – such as those we have mentioned – will be crucial.

5.10 The Criminal Offences Gateway Guidance – which implemented, in large part, our Consultation Paper on Criminal Liability in a Regulatory Context[360] – includes factors to consider when deciding whether a new criminal offence is appropriate. When considering proposals for a new criminal offence, the Secretary of State for Justice will, according to the Criminal Offences Gateway Guidance, consider (amongst others) the following matters:

(1) whether the behaviour is sufficiently serious to merit the stigma associated with a criminal conviction;

(2) whether the behaviour is already caught by the existing criminal law; and

(3) the formulation of the individual offences proposed, in particular to consider whether they focus on the behaviour being targeted without criminalising behaviour more widely – this will require consideration of the individual elements of the offence (the conduct, any mental element and any defences).[361]

---

357 Online Harms White Paper (2019) CP 57. The Government have published an initial consultation response, publish 12 February 2020 (full response to follow), https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response (last visited 09 September 2020).

358 See, for example, YouTube, *Community Guidelines*, available at https://www.youtube.com/about/policies/#community-guidelines (last visited 13 November 2019) and Twitter, *The Twitter Rules*, available at https://help.twitter.com/en/rules-and-policies/twitter-rules (last visited 13 November 2019).

359 I Ahmed and L Papadopoulos, *Don't Feed the Trolls: How to Deal with Hate on Social Media,* https://252f2edd-1c8b-49f5-9bb2-cb57bb47e4ba.filesusr.com/ugd/f4d9b9_ce178075e9654b719ec2b4815290f00f.pdf (last visited 09 September 2020).

360 Criminal Liability in a Regulatory Context (2010) Law Comm No 195.

361 Ministry of Justice, *Criminal Offences Gateway Guidance*.

5.11 Regarding the first consideration, we must be careful to ensure that harmful but non-culpable behaviour is not caught by our proposed new communications offences. Not all harmful behaviour is sufficiently serious to merit the stigma associated with criminal conviction. Indeed, some harmful behaviour is permissible or even desirable. This is true of online communications as it is all other fields of human activity. Consider, for example, a highly effective online advertising campaign for a new brand of eco-friendly, ethically produced sports clothing. Such a campaign may harm the new brand's competitors, but is – all things being equal – at least permissible or even desirable.

5.12 Other, more pertinent examples include an iMessage delivering news of the death of a family member or a post by a recent divorcee, announcing their new relationship. In both of these examples, the communication may cause serious emotional distress – to the bereaved individual or to the divorcee's former partner. But such communications should not, without more, be criminal. We discuss such examples below, at 1.163-1.164.

5.13 Regarding the second and third considerations, it will be important to ensure that any new communications offence is not overly broad. A new communications offence should be targeted so as to cover the worst instances of abusive online communications, while ensuring minimal overlap with existing offences covering different types of conduct.

### Technological neutrality

5.14 The offence under section 127 of the Communications Act 2003 ("CA 2003") applies only to communications made via a public communications network (for a full discussion see Chapter 3). This makes the offence too narrow to cover some forms of online communication, particularly communication via Bluetooth, AirDrop, or other peer-to-peer services. It also makes the offence badly targeted: if the intention is to protect members of the public from receiving abusive communications, why criminalise only one mode of communication (that is, communication via a public network); one that is not qualitatively distinct from other forms of communication? An abusive communication is not necessarily less abusive, or harmful, when sent via a peer-to-peer network, rather than via the internet.

5.15 Section 1 of the Malicious Communications Act 1988 ("MCA 1988") covers a broader range of modes of communication. A "communication" includes an "electronic communication", which covers online communications and communications via peer-to-peer services. In our view, the new communications offence should be the same in scope as the section 1 MCA 1988 offence: it should cover any letter, electronic communication (such as internet-based communications), and article of any description (a definition that would include items such as faeces or used tampons). In what follows, we explain our reasoning.

#### Digital or online communications only?

5.16 One alternative would be to limit the scope of the new offence(s) to "digital" or "online" communications only. Some jurisdictions, such as New Zealand, have taken this kind of approach. New Zealand's Harmful Digital Communications Act 2015 ("HDCA 2015") applies exclusively to "digital" communications.

5.17 The HDCA 2015 contains both a civil complaints regime and a criminal offence, and was enacted specifically to respond to "cyberbullying". Its ten principles include, for example, that a digital communication should not be grossly offensive to a reasonable person in the position of the affected individual; threatening, menacing or intimidating; or indecent or obscene. These ten principles apply only to digital communications.[362]

5.18 Under section 4 of the HDCA 2015, a "digital communication" is:

> (a) any form of electronic communication; and
>
> (b) includes any text message, writing, photograph, picture, recording, or other matter that is communicated electronically.

5.19 The HDCA 2015 arose out of the New Zealand Law Commission's Ministerial Briefing Paper on Harmful Digital Communications. In that paper, the New Zealand Law Commission acknowledged the view that "laws should reflect broad principles which are capable of being applied in a technology-neutral manner".[363] However, this view was deemed "too simplistic":[364]

> For the first time in history, individuals with access to basic technology can now publish, anonymously, and with apparent impunity, to a potentially mass audience. This facility to generate, manipulate and disseminate digital information which can be accessed instantaneously and continuously is producing types of abuse which have no precedent or equivalent in the pre-digital world.
>
> In our view the resulting emotional harms that can arise from the misuse of digital communication technologies are of such a serious nature as to justify a legal response.[365]

5.20 As a result, the New Zealand Law Commission recommended "a new criminal offence tailored for digital communication".[366] Regarding the choice of the term "digital", as opposed to "online", there was no discussion of the relative merits of the two. However, regarding the relevant features of the former, the New Zealand Law Commission said this:

---

362 Harmful Digital Communications Act 2015 (New Zealand), s 6.

363 New Zealand Law Commission, *Ministerial Briefing Paper on Harmful Digital Communications: the adequacy of the current sanctions and remedies* (August 2012) at para 1.35.

364 New Zealand Law Commission, *Ministerial Briefing Paper on Harmful Digital Communications: the adequacy of the current sanctions and remedies* (August 2012) at para 1.35.

365 New Zealand Law Commission, *Ministerial Briefing Paper on Harmful Digital Communications: the adequacy of the current sanctions and remedies* (August 2012) at para 1.35-1.36.

366 New Zealand Law Commission, *Ministerial Briefing Paper on Harmful Digital Communications: the adequacy of the current sanctions and remedies* (August 2012) at p 11.

> The distinguishing feature of electronic communication is that it has the capacity to spread beyond the original sender and recipient, and envelop the recipient in an environment that is pervasive, insidious and distressing.[367]

5.21 Ireland's Law Reform Commission has taken a different approach. In their Harmful Communications and Digital Safety Report, they recommended that "the legislation included in this Report should apply to all forms of communication, whether offline or online, analogue or digital".[368] Their recommendations have not yet been implemented but form the basis of the Harassment, Harmful Communications and Related Offences Bill 2017, which is currently progressing through the legislative process.

5.22 The recommendations made by Ireland's Law Reform Commission were informed by a number of "principles of reform", including the principle of technological neutrality.[369] The various permutations of this principle were noted. For example, on one interpretation of the principle, identical rules apply both online and offline. Alternatively, on another interpretation, different rules apply online and offline, with the aim of realising an equivalent effect.

5.23 Ultimately, the approach taken in the Harmful Communications and Digital Safety Report, and in the 2017 Bill, is for all the relevant offences (covering harassment, stalking, and certain one-off communications) to apply to communication *by any means*; including, but not limited to, online and digital communications. Hence, it is clear that two very different approaches have been taken by different jurisdictions in recent years, regarding the question of whether or not to have technologically specific (online-only or digital-only) communications offences.

5.24 The HDCA 2015 has been criticised for making "an arbitrary distinction between the online and offline worlds".[370] Criticism along these lines was noted by Ireland's Law Reform Commission in their report.[371] Similarly, Professor Ursula Cheer, in comparative analysis requested by us as part of the scoping phase of this project, describes it as "unfortunate" that "New Zealand's criminal laws now support different

---

367 New Zealand Law Commission, *Ministerial Briefing Paper on Harmful Digital Communications: the adequacy of the current sanctions and remedies* (August 2012) at p 17.

368 Ireland Law Reform Commission *Report on Harmful Communications and Digital Safety* (LRC 116-2016) at para 2.53.

369 Ireland Law Reform Commission *Report on Harmful Communications and Digital Safety* (LRC 116-2016), at paras 1.83-1.87.

370 D Gambitsis, *Cross-Examination: The Unintended Consequences of the Harmful Digital Communications Act* (22 July 2015), https://www.equaljusticeproject.co.nz/blog/2015/07/cross-examination-the-unintended-consequences-of-the-harmful-digital-communications-act (last visited 10 December 2015).

371 Ireland Law Reform Commission *Report on Harmful Communications and Digital Safety* (LRC 116-2016) at 2.114, citing G Hughes, *New law poorly-drafted, vague, and could criminalise free speech* (03 July 2015), https://www.stuff.co.nz/the-press/opinion/69955436/new-law-poorly-drafted-vague-and-could-criminalise-free-speech (last visited 09 December 2019).

approaches to online and offline speech",[372] with the former being regulated more strictly than the latter.

5.25 We can see two related problems with a technologically-specific approach. The first relates to futureproofing: we are sceptical about the possibility of finding a satisfactory definition of "digital" or "online" that would be sufficiently flexible to accommodate new and unforeseeable technological developments. Communications made using such new technologies may well be appropriate for criminal regulation, but may fall outside any definition of "online" and "digital" upon which we settle. This problem is especially acute given that, according to some prominent theorists such as Ray Kurzweil, the rate of technological change is exponential.[373] If this is right, a significant and unforeseeable change to communication technology could be imminent.

5.26 It will be recalled that the section 127 CA 2003 offence criminalises conduct that is not obviously wrong, such as sexting or storing images or communications in the cloud, as well as under-criminalising conduct that happens not to use a public communications network. By replacing "public communications network" with "online", we risk essentially replicating the error, namely creating an offence whose scope is rendered inappropriate by technological change.

5.27 This first problem points toward a second and deeper problem: namely, that no plausible definition of "online" or "digital" captures the pertinent attributes of these types of communication which tend to make them worthy of a specific criminal law response (as against, say, oral, face-to-face communication).

5.28 Section 4 of the HDCA 2015 defines digital communication as "any form of electronic communication". In our view, the fact that a message is sent electronically does not give rise to a specific and separate type of harm, such that these communications warrant a specific criminal law response. It is necessary to create an offence that adequately captures within its scope those behaviours that are qualitatively similar, without creating an offence so specific that it can be easily circumvented. This is part of the reason for having an offence that is, so far as possible, technologically neutral.

5.29 Similar, and potentially more significant, problems arise with making "online" a requirement. In our Scoping Report, we defined "online communication" as "communication via the internet"; by contrast, "offline communication" was defined as "communication that does not use the internet".[374] On this definitional scheme, online communications would include, for example, an iMessage but not a text message. But making the former subject to specific criminal regulation and not the latter seems arbitrary – especially given that, from an iPhone user's perspective, these two modes of communication can be almost indistinguishable. Hence, "online", defined in this way, is probably under-inclusive.

---

372 Professor Ursula Cheer, *Abusive and Offensive Communications: the criminal law of New Zealand,* https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/11/New-Zealand-U-Cheer.pdf, at para 1.1.

373 See for example R Kurzweil, *The Singularity is Near* (2016).

374 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at p viii.

5.30 This may suggest that the appropriate target of special regulation is not "online" or "digital" communications as such, but communications that share some other characteristics. It will be useful, then, to consider the attributes that online communications are generally taken to possess, such that they may (perhaps mistakenly) be thought to warrant special regulation.

### Are there distinctive characteristics of online communications?

5.31 The New Zealand Law Commission noted the following "critical features" of "digital" communication which, they said, distinguish it from "offline" communication:

(1) The viral nature of cyberspace and the potential for information to be disseminated instantly to worldwide audiences;

(2) The ubiquity of the technology which means communications are no longer constrained by time and place but can be accessed anywhere, anytime by anyone;

(3) The persistence of information disseminated electronically;

(4) The ease with which digital information can be accessed/searched;

(5) The facility for anonymous communication and the adoption of multiple online personae.[375]

5.32 Similar distinguishing features of "digital" or "online" communications have been identified elsewhere. For example, quoting from the 2010 film, *The Social Network,* Advocate General Szpunar of the Court of Justice of the European Union opened a recent opinion by noting that "the internet's not written in pencil, it's written in ink".[376] In other words, online communications are generally considered to be more permanent than their offline counterparts.

5.33 Dr Laura Scaife, author of *Handbook of Social Media and the Law*, also identifies permanence as a distinguishing feature of online communications, particularly via social media. She further notes that these communications are often one-to-many rather than one-to-one, are spontaneous, and have a greater reach and degree of accessibility.[377]

5.34 Whilst we recognise that online communications tend to have a greater permanence and reach than offline communications, it is – at least arguably – these characteristics that are of concern, not the plain fact that the communication is online. And this is a *tendency* rather than a rule. Indeed, while permanence and reach may be properly understood as features of the social media paradigm embodied by platforms like

---

375 New Zealand Law Commission, *Ministerial Briefing Paper on Harmful Digital Communications: the adequacy of the current sanctions and remedies* (August 2012), at p 38.

376 Opinion of the Advocate General Szpunar, Case C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited* [2019] ECR I-458, at [1].

377 See, for example, L Scaife, *Handbook of Social Media and the Law* (2015), at p 5.

Facebook and Twitter, other online communications tools, such as Snapchat, have moved away from this model.

5.35 Snapchat's self-destructing photo and video messages ("snaps") are deliberately ephemeral: when Snapchat launched, this was its unique selling point. Communications via Skype and FaceTime are even more transient. While a snap is stored on the recipient's phone until it is opened, video calls over Skype and FaceTime take place in real time without this period of storage on the recipient's device. Moreover, snaps, along with many other types of online communication (particularly in the form of email, WhatsApp messages, or iMessages), can be one-to-one, as well as one-to-many: they are often messages sent to a single recipient.

5.36 Equally, it is possible that an offline communication could have a high degree of permanence, reach, and accessibility – consider, for example, a billboard in Parliament Square which may exist for a lengthy period and be viewed by many passers-by.

5.37 Dr Alexander Brown has canvassed various other candidates for the distinctive feature of online communications, some of which overlap with the fifth feature identified by the New Zealand Law Commission (above at 1.31). These are: anonymity (of the speaker); invisibility (of both the speaker and the audience); instantaneousness or spontaneity; and degree or type of harm (the former, Brown observes, possibly being a function of the permanence of the communication).

5.38 Ultimately, Brown argues that

> the supposed anonymity of the Internet may not be as distinctive as is first assumed but… the instantaneous nature of some parts of the Internet and the spontaneous hate speech that it encourages might be a better, and often overlooked, reason to mark it out as different.[378]

5.39 However, even if it is true that anonymity – and lack of physical proximity – of the online environment encourages, or is conducive to, certain kinds of harmful speech (such as hate speech), we are not convinced that this is sufficient to require that "online" be an ingredient of a criminal offence. In short, there seems to be no principled reason for creating a separate regime for digital or online communications.

### Repealing and replacing section 127(1) of the Communications Act 2003 and the Malicious Communications Act 1988

5.40 In light of the foregoing, our view is that the new communications offence should be the same in scope as the offence under section 1 MCA 1988: it should cover any letter, electronic communication, or article (of any description). This avoids making an arbitrary distinction between online communications and other, qualitatively similar forms of electronic communication (such as iMessages and text messages). It will also mean that we avoid incentivising a switch to offline modes of abuse, such as the use

---

[378] A Brown, 'What is so special about online (as opposed to offline) hate speech?', 18(3) *Ethnicities* 297, at p 320.

of “services” which send items such as used condoms, used tampons, or faeces to a target.[379]

5.41 Given its scope, the proposed new offence is suitable to replace the offence under the MCA 1988. It is also, we think, suitable to replace the offence under section 127(1) CA 2003 which applies only to communications sent via a public network and is in this respect narrower than the offence under the MCA. In our view, the proposed new offence should, like the offence under the MCA, be triable either-way.

5.42 We do not think, however, that the proposed new offence should replace section 127(2) CA 2003, which covers knowingly false communications. In Chapter 6, in which we set out proposals for complementary law reforms, we explain our proposed amendments to section 127(2).

### A harm-based model

5.43 When considering how to reform the communications offences to address more effectively abusive online communications, we considered various alternatives. Three of the main options we considered were:

(1) providing a statutory definition of “grossly offensive”;

(2) replacing some or all of the existing proscribed characteristics with a new characteristic: “abusive”;

(3) replacing the existing communications offences with a new offence based on potential for harm.

5.44 Our provisional view is that the third option – a harm-based model – is the best approach. In what follows, we explain the reasoning behind this view.

5.45 The MCA 1988 and section 127(1) CA 2003 criminalise communications, the character of which is described using certain adjectives: “indecent”, “menacing”, or “grossly offensive.” As we explain in Chapter 3, we see the merits of this model. However, it also suffers from serious problems. Again, these are set out in full in Chapter 3 but, for convenience, we summarise them here.

5.46 One of the main problems, especially with the term “grossly offensive” is that it is vague and may therefore fall foul of Article 10 ECHR. CPS guidance has, to an extent, clarified the term. However, it is not satisfactory to rely on prosecutorial discretion to limit the scope of the offence. One possible solution would be to provide a statutory definition of “grossly offensive”, which could reflect the CPS guidance in substance, but which would have the status of law. This would not, however, solve the additional and more serious problem that such adjectives are not sufficiently (nor even necessarily) congruent with harm. A grossly offensive communication may be harmful but, equally, may not.

5.47 Another option would be replacing some or all of the existing proscribed characteristics with a new characteristic: “abusive”. However, we found that all of the

[379] This example was giving to us by Refuge in a pre-consultation meeting.

workable definitions of “abusive” that we considered were essentially proxies for a combination of harm and fault.

5.48 We therefore propose that, instead of using such adjectives, a new offence should be based on the potential of the communication to cause harm. This approach, will, in our view, help to avoid the dual problems of over- and under-criminalisation suffered by the existing offences, create a better targeted offence, and serve as a clearer guide for behaviour.

## THE PROPOSED OFFENCE SUMMARISED

5.49 The elements of our proposed new communications offence can be summarised follows:

(1) The defendant sends or posts a communication that was likely to cause harm to a likely audience;

(2) in sending or posting the communication, the defendant intended to harm, or was aware of a risk of harming, a likely audience; and

(3) the defendant sends or posts the communication without reasonable excuse.

(4) For the purposes of this offence, definitions are as follows:

(a) a **communication** is a letter, electronic communication, or article of any description;

(b) a **likely audience** is someone who, at the point at which the communication was sent or posted by the defendant, was likely to see, hear, or otherwise encounter it; and

(c) **harm** is emotional or psychological harm, amounting to at least serious emotional distress.

(5) When deciding whether the communication was likely to cause harm to a likely audience, the court must have regard to the context in which the communication was sent or posted, including the characteristics of a likely audience.

(6) When deciding whether the defendant had a reasonable excuse for sending or posting the communication, the court must have regard to whether the communication was, or was meant as, a contribution to a matter of public interest.

**Consultation Question 1.**

5.50 We provisionally propose that section 127(1) of the Communications Act 2003 and section 1 of the Malicious Communications Act 1988 should be repealed and replaced with a new communications offence according to the model that we propose below. Do consultees agree?

5.51 By way of summary (though we make separate proposals in respect of each of these below), the elements of the provisionally proposed offence are as follows:

(1) The defendant sent or posted a communication that was likely to cause harm to a likely audience;

(2) in sending or posting the communication, the defendant intended to harm, or was aware of a risk of harming, a likely audience; and

(3) the defendant sent or posted the communication without reasonable excuse.

(4) For the purposes of this offence, definitions are as follows:

(a) a **communication** is a letter, article, or electronic communication;

(b) a **likely audience** is someone who, at the point at which the communication was sent or posted by the defendant, was likely to see, hear, or otherwise encounter it; and

(c) **harm** is emotional or psychological harm, amounting to at least serious emotional distress.

(5) When deciding whether the communication was likely to cause harm to a likely audience, the court must have regard to the context in which the communication was sent or posted, including the characteristics of a likely audience.

(6) When deciding whether the defendant had a reasonable excuse for sending or posting the communication, the court must have regard to whether the communication was, or was meant as, a contribution to a matter of public interest.

5.52 Below, we discuss in detail the reasoning behind each of the elements of the proposed offence. First, though, we set out for comparison the offence under New Zealand's Harmful Digital Communications Act 2015 ("HDCA 2015"),[380] to which some aspects of our proposed new offence are indebted. Given that the New Zealand

[380] Harmful Digital Communications Act 2015 (New Zealand).

offence, like our proposed new offence, is a harm-based model, it has been a particularly useful comparator.

### The New Zealand Model

5.53 Section 22 of the HDCA 2015 provides:

> (1) A person commits an offence if—
>
> (a) the person posts a digital communication with the intention that it cause harm to a victim; and
>
> (b) posting the communication would cause harm to an ordinary reasonable person in the position of the victim; and
>
> (c) posting the communication causes harm to the victim.
>
> (2) In determining whether a post would cause harm, the court may take into account any factors it considers relevant, including—
>
> (a) the extremity of the language used;
>
> (b) the age and characteristics of the victim;
>
> (c) whether the digital communication was anonymous;
>
> (d) whether the digital communication was repeated;
>
> (e) the extent of circulation of the digital communication;
>
> (f) whether the digital communication is true or false;
>
> (g) the context in which the digital communication appeared.
>
> (3) A person who commits an offence against this section is liable on conviction to—
>
> (a) in the case of a natural person, imprisonment for a term not exceeding 2 years or a fine not exceeding $50,000;
>
> (b) in the case of a body corporate, a fine not exceeding $200,000.
>
> (4) In this section, **victim** means the individual who is the target of a posted digital communication.[381]

5.54 Under section 4, key terms are defined as follows:

> (1) **posts a digital communication**—

[381] Harmful Digital Communications Act 2015 (New Zealand), section 22.

(a) means transfers, sends, posts, publishes, disseminates, or otherwise communicates by means of a digital communication—

(i) any information, whether truthful or untruthful, about the victim; or

(ii) an intimate visual recording of another individual; and

(b) includes an attempt to do anything referred to in paragraph (a).

(2) **digital communication**—

(a) means any form of electronic communication; and

(b) includes any text message, writing, photograph, picture, recording, or other matter that is communicated electronically.

(3) **harm** means serious emotional distress.[382]

5.55 The proposed new offence is similar to the offence under section 22 HDCA 2015 in several respects. Both offences can be described as "harm-based" models. The threshold of harm is, in both cases, serious emotional distress and both offences include factors to consider when establishing the harmfulness of the communication. Both offences also include a significant mental element.

5.56 However, despite their similarities, there are some important differences between the two models. First, section 22 HDCA 2015 only covers a relatively narrow range of content: the definition of "posts a digital communication" limits the scope of the offence to "any information, whether truthful or untruthful, about the victim" or "an intimate visual recording of another individual".[383]

5.57 Second, while the section 22 HDCA 2015 offence covers only digital forms of communication, our proposed offence covers both electronic and some non-electronic communications.

5.58 Third, the harm requirements are different. The harm requirement under the section 22 HDCA 2015 is an *actual* harm requirement: the victim must actually be harmed by the communication. In addition to this subjective element of the harm requirement, there is also an objective element: "posting the communication would cause harm to an ordinary reasonable person in the position of the victim". Our proposed offence has no such actual harm requirement. Instead, the offence is complete when the defendant sends or posts a communication *likely* to cause harm (that is, emotional or psychological harm amounting to at least serious emotional distress) to someone likely to see, hear, or otherwise encounter it.

---

382 Harmful Digital Communications Act 2015 (New Zealand), section 4.

383 Admittedly, "information about the victim" has, in some cases, been interpreted broadly. For example, in *Whitmore v Police* [2019] NZDC 23935, the defendant was convicted of causing harm by posting a digital communication after he sent threatening voice recordings via Facebook to his daughter saying, for example, that she "was no longer a part of [his] family," and that if she did not stay away from the family he would "slit her throat".

5.59 Fourth, the proposed new offence does not include a list of factors for the court to consider when establishing harm: it stipulates only that the court must consider the context in which the communication was sent or posted, including the characteristics of a likely audience.

5.60 Finally, the proposed new offence encompasses conduct where the mental element is awareness of a risk rather than intent. This reflects our view that some abusive communications should be criminal, even though there is no intention to cause harm. Where there is intention to cause harm, there may be higher degree of culpability and this should be reflected at sentencing.

5.61 In what follows, we explain reasoning for these divergences and, more generally, the reasoning behind each element of the proposed offence.

## THE CONDUCT ELEMENT

5.62 The conduct element of the new offence should, we propose, be as follows: a person commits an offence if they send or post a communication likely to cause harm to a likely audience, where "harm" is defined as emotional or psychological harm amounting to at least serious emotional distress, and "a likely audience" is someone who, at the time the communication was sent or posted, was likely to see, hear, or otherwise encounter it.

### "Sent or posted a communication"

5.63 Under section 1 MCA 1988, the conduct element covers both electronic communications (such as communications sent via the internet) and non-electronic communications. In our provisional view, the proposed new offence should be aligned with the section 1 MCA offence in this regard. The proposed new offence thereby avoids the pitfalls of the section 127 CA offence in criminalising only certain forms of electronic communication. It also differs from the section 22 HDCA 2015 offence in that it is not limited to digital communications and avoids the problems of a "technologically specific" approach.

5.64 However, in another respect, the proposed offence expands on the forms of communication covered under section 1 MCA 1988. As we explain in Chapter 2, the offence under section 1 MCA 1988 requires that the defendant sends a communication of the proscribed character *to an intended recipient*. Our proposed offence has no such requirement. It would cover posts on social media, such as a publicly available Tweet or a comment below an online newspaper article, both of which have no intended recipient and are accessible to the world at large. Such communications may technically be covered by the word "sent"[384] but, for the sake of clarity, we have added the word "posted".

5.65 Examples of "sending or posting" that would be covered by the proposed offence include: emailing; sending via other internet-enabled instant messages (such as iMessages, WhatsApp messages, and direct messages on Instagram or Facebook

[384] Under the New Zealand legislation, the reverse is also true: the word "posts" is defined to include "sending" – see above at 1.53.

Messenger); sending text messages; posting on social media platforms (such as Twitter, Facebook, Instagram, and YouTube) and blogs, whether such posts are publicly available or available only to the poster's "friends" or "followers"; communicating via VoIP (such as Skype calls, WhatsApp calls, or Google calls);[385] and sending letters or items via the Royal Mail and other postal services. A "communication" is a letter, article, or electronic communication, and could be: written words; images; audio; video; or items like used condoms, used tampons, or faeces.

5.66 We do not, however, intend for the proposed offence to cover regulated media such as the news media, broadcast media, and cinema. Our intention is that the publisher of an online newspaper article would not be caught by the proposed offence, but an individual who posts an abusive comment in response to the article would be caught. This could be achieved by way of a carve out, if necessary.

5.67 There are several reasons for this. Firstly, if these forms of communication were to be covered, this would dramatically expand the scope of the existing communications offences in a way that we do think is justified and which goes significantly beyond our Terms of Reference. Further, given that a free and independent press is crucial in a democratic society, the burden of justification for imposing criminal liability (where none currently exists) is especially weighty. Even if there were not, in fact, any successful prosecutions of the press under the proposed offence, there is a risk that mere existence of the offence would have a chilling effect on the exercise of freedom of expression by the press and media outlets. Finally, the existing regulatory schemes[386] within which these groups operate render the imposition of additional criminal liability superfluous.

**Consultation Question 2.**

5.68 We provisionally propose that the offence should cover the sending or posting of any letter, electronic communication, or article (of any description). It should not cover the news media, broadcast media, or cinema. Do consultees agree?

### "A likely audience"

5.69 As we explain above, the offence under section 1 MCA 1988 is limited in that it only covers situations where there is an intended recipient. It does not cover communications posted in a public forum, such as the comments section below an online newspaper article or public Tweets (posts on Twitter that are visible to anyone, whether or not they have a Twitter account).

5.70 The proposed new offence, by contrast, encompasses potential harm to anyone who was, at the time the communication was sent or posted by the defendant, likely to see, hear or otherwise encounter it. This makes it capable of covering communications

---

385 VoIP is an acronym from Voice over Internet Protocol.

386 Newspapers and magazines are primarily regulated by IMPRESS and the Independent Press Standards Organisation. Television and radio are regulated by Ofcom. Cinema is regulated by the British Board of Film Classification.

posted to a mass, unspecified audience. Similarly, the mental element under the proposed new offence is intention or awareness of a risk of causing harm to someone likely to see, hear, or otherwise encounter the communication. Here again, the offence is broader than section 1 MCA 1988, which requires intention to harm a particular recipient.

5.71 A key aspect of the justification for encompassing anyone who is likely to see, hear, or otherwise encounter the communication is that – as academics such as Bakalis have pointed out – the harm of online communications, particularly online hate, can extend beyond those towards whom the communication is directed. Bakalis enumerates three types of "bystander" to online hate. In relation to the proposed new offence, two of the three types are relevant. The first type is bystanders who share the characteristics of those towards whom the communication is directed. The second type is bystanders who come across hateful material or watch as online hate unfolds. People in both of these categories can be harmed, even if they are not directly targeted by the communication.[387]

5.72 Further, as we explain in Chapter 4, doxing and outing are forms of online abuse about which certain stakeholders, such as Galop and Refuge, have expressed particular concern. By "doxing", we mean the sharing of private or identifying information about a particular individual without their consent. "Outing" is a specific form of "doxing", where the information shared concerns an aspect of the individual's identity such as their gender identity, sexual orientation, or HIV status.[388] Doxing and outing may take place by way of written information (such as a home address, phone number, or statements about a person), audio recordings of a person, images, or videos.

5.73 The primary victim of these forms of online abuse is the person whose information is shared (as a shorthand, we will call this person the "information subject"). The information subject may not be the direct recipient of the communication nor one of the perpetrator's followers on social media. Nonetheless, in many cases, they will be likely to suffer emotional or psychological harm amounting to at least serious emotional distress as a result of the perpetrator's communication.

5.74 For the purposes of our proposed offence, it does not matter that the information subject is not a recipient of the communication. Nor does it matter whether the information subject in fact sees the communication. If, at the time the perpetrator sent or posted the communication, the information subject was *likely* to see, hear, or otherwise encounter it (because, say, a mutual friend was likely to show it to them), the perpetrator's conduct could be covered by the proposed offence (as long as the other elements are made out). Consider the following example:

---

387 C Bakalis, "Rethinking cyberhate laws, Information & Communications Technology Law" (2018) 27(1) *Information & Communications Technology Law* 86, at p 104. The third type of bystander is one who might be influenced or radicalised by their exposure to online hate.

388 See L Hubbard, *Online Hate Crime Report* (Galop 2020), http://www.galop.org.uk/online-hate-crime-report-2020/ (last visited September 2020), at p 7.

**Example 1: outing**

Alvin and Asmita met on a dating app. Alvin quickly broke things off when he found out that Asmita is a transgender woman. Asmita told Alvin that very few people in her life know about her transition.

Alvin finds Asmita's colleagues on LinkedIn and uses the LinkedIn messenger service to send them photos of Asmita, with captions like, "Take a closer look…THIS IS NOT A WOMAN, THIS IS AN EFFING MAN! You work with a pervert freak. Just thought you'd want to know. Tell HIM Alvin says hi". Concerned, one of Asmita's colleagues shows her the messages.

5.75 It is arguable that Asmita was, at the point at which Alvin sent the messages, likely to encounter them. This is on the grounds that a colleague was likely to bring them to her attention. Indeed, especially given that the message ended by saying "Tell HIM Alvin says hi", it seems that this was Alvin's intention. It seems that he intended, or was at least of aware of a risk, that Asmita would encounter the messages and thereby be caused harm. Even without the final sentence of the message, there would be a strong argument that Asmita was likely to encounter the messages (and that Alvin intended or was aware of a risk that she would). Alvin's abusive behaviour is directed at Asmita; the point is that the behaviour will have a harmful impact on her and it was therefore likely she would at some point encounter the messages, albeit through the mediation of a third party.

5.76 Hence, as the example illustrates, the "likely audience" requirement would allow for doxing and outing to be prosecuted under the proposed offence. However, unlike the New Zealand offence – which explicitly refers to intimate visual recordings of and information (whether truthful or untruthful) about the "target" of the communication – our proposed offence does not squarely address doxing, outing, and other forms of sharing of personal content as its central concern. The proposed offence does not necessarily reflect the nature of the harmful conduct, which may be better understood as, for example, a privacy violation. While a victim of such conduct will often be likely to see the communication, we accept that this is not necessarily the primary harm. Therefore, it may be that – at least in some cases, such as the sharing of sexual images without consent – there is a need for a better-targeted offence. This is explored in more detail in the Law Commission's separate project on the taking, making, and sharing of intimate images without consent.[389]

5.77 We note that an alternative approach would be to remove the "likely audience" requirement and instead to create an offence that could be committed if the communication was likely to cause harm to any person. However, in our provisional view, the "likely audience" restriction is necessary to ensure that the offence is not overly broad. We have reservations about creating an offence that covers remote

[389] Information on the Law Commission's Consultation Paper on taking, making, and sharing of intimate images without consent is available at www.lawcom.gov.uk.

harms, which do not have a sufficient causal connection with the defendant's conduct. The "likely audience" requirement helps to prevent this.

5.78 Another option would be to extend this element of the offence to include two alternatives: the communication was likely to cause harm to a likely audience *or to the information subject.* On this approach, the offence would cover a communication that harms the information subject, but that they did not and were not likely to encounter. For example, it might cover damaging lies about the information subject, told in secret to a potential employer or business partner.

5.79 Here again, we have concerns about the breadth of such an offence and its propensity to cover remote harms (though we accept that the cause for concern is weaker than if we simply did away with the likely audience requirement without replacement). Further, extending the proposed offence to cover harm to the information subject would go well beyond the scope of the existing communications offences. It seems to us that it is in the nature of the existing communications offences that they address direct harm to someone likely to encounter the communication (albeit that they do so inadequately). Harm to the information subject is addressed in civil law by, for example, the tort of defamation – defamation having been decriminalised in 2009.[390] In a narrow range of cases, notably the sharing of sexual images without consent, a criminal offence may be appropriate even when the person depicted does not encounter the images. But creating an offence which covers, in general, communications likely to cause harm to the information subject would, in our provisional view, be an unjustified extension of the existing communications offences.

5.80 One question that arises is whether the assessment of who counts as a "likely audience" for the purposes of the offence – that is, who was likely to see, hear, or otherwise encounter the communication – should be objective or subjective. In our view, when establishing whether the conduct element of the offence was met, the test should be objective. The question should be whether the communication was, as a matter of fact, likely to cause harm to someone who, as a matter of fact, was likely to see, hear, or otherwise encounter it. This can be balanced with a subjective test when establishing the mental element. At that stage, the question is whether the defendant intended or was aware of a risk of harm to someone likely to see, hear, or otherwise encounter the communication. To reach an affirmative answer, the court must have in mind those people who, in the defendant's view, were likely to see, hear, or otherwise encounter the communication.

5.81 In many cases, the objective and subjective tests for "a likely audience" will produce the same result. For example, if a defendant sends an abusive iMessage to her ex-partner then, all things being equal, the defendant's ex-partner is, objectively and subjectively, likely to see the iMessage. If, on the other hand, the defendant is a celebrity with a large Twitter following, and she posts an abusive Tweet, then the number of people likely to see the message is, objectively and subjectively, much larger.

---

390 Section 73 of the Coroners and Justice Act 2009 abolished the common law offences of: sedition and seditious libel; defamatory libel; and obscene libel.

**Consultation Question 3.**

5.82 We provisionally propose that the offence should require that the communication was likely to cause harm to someone likely to see, hear, or otherwise encounter it. Do consultees agree?

### "Likely" harm, not actual harm

5.83 The harm requirement under section 22 HDCA 2015 has both a subjective and an objective element. The subjective element is that a victim was actually harmed. In our view, a new communications offence should have no such requirement. Instead, the proposed new offence requires the prosecution to show that harm was likely to be caused to someone likely to see, hear, or otherwise encounter the communication.

5.84 The main advantages of this are:

(1) the offence is capable of covering communications that have the potential to cause harm, but did not actually cause harm, or where it is not known whether they caused harm; and

(2) the victim does not have to go through the potentially re-traumatising process of producing evidence that they were harmed.

5.85 Regarding the first of these two points, proof of harm may be especially difficult to obtain in the case of public posts, where it is difficult to establish who has seen the communication. Further, given the culture of dismissiveness and normalisation around harmful online communications (see Chapters 3 and 4), victims may be especially unlikely to come forward.

5.86 An important consideration is the threshold to set in respect of the risk of harm. In our proposal, the threshold is crossed if the communication was *likely* to cause harm to a likely audience. But there are, of course, alternatives.

5.87 One alternative is to set a "*de minimis"* threshold: this is a legal term meaning too small to be meaningful or taken into consideration. It is taken from a longer Latin phrase which translates into "the law does not concern itself with trifles." On this alternative, the threshold would be crossed provided that the risk of harm posed by the communication was material or non-trivial.

5.88 In our provisional view, the conduct element should specify that the communication was likely to cause harm, rather than that the risk of harm was material or non-trivial. Otherwise, the conduct element would be too easily met and the connection with harm would be too loose.

5.89 We also note that a "likelihood" threshold is used in comparable offences under the Public Order Act 1986. For example, under section 5 of the POA 1986, a person is guilty of an offence if they 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.

5.90 One remaining question is how the prosecution would establish that a communication was likely to cause harm. In our view, evidence that an actual victim was harmed would count towards this, but may not be determinative. This is because, in some cases, it may be that a small risk of harm so happened to eventuate. In our view, it may be helpful to include factors for the court to take into account in deciding whether harm was likely. We discuss this further below, at 1.117-1.120.

**Consultation Question 4.**

5.91 We provisionally propose that the offence should require that the communication was likely to cause harm. It should not require proof of actual harm. Do consultees agree?

### Categories of harm: emotional or psychological harm

5.92 As we explain in Chapter 4, we think there is a strong justification for limiting the proscribed categories of harm to emotional and psychological harms. By limiting the definition of "harm" in this way, we prevent the offence from becoming overly broad. An act of communication could cause many different types of harm in many different ways, but not all of these behaviours fall within the proper scope of a project, or offence, addressing abusive online communications.

5.93 To put it another way, our view is that not all harmful communications should be criminalised under a single set of offences. Currently there are different offences covering bribery, harassment, fraud, and stirring up hatred. A new set of offences should not be so broad as to cover all of these behaviours, and more. As we set out in Chapter 4, many abusive communications are unified by their propensity to cause emotional or psychological harm directly to someone who sees them. A new offence should, in our view, be targeted at such communications.

5.94 Consider, for example, fraud. If we include economic harm in the definition, then the proposed new offences would probably cover fraud. This would be especially problematic given that, in our Consultation Paper on Criminal Liability in a Regulatory Context, which was later implemented in large part by the Ministry of Justice in the form of the Criminal Offences Gateway Guidance, we proposed that the criminal law should not be used to deal with fraud when the conduct in question is covered by the Fraud Act 2006. Of course, we are in no way suggesting that these hypothetical new communications offences would make the Fraud Act and associated jurisprudence redundant or even that they would end up playing any significant role in the prosecution of fraud. However, this example does illustrate the troubling consequences of including economic harm in the definition of "harm": the offences would be so broad that they would in theory catch fraud or fraud-like behaviour.

5.95 In short, there are, as we set out in the Scoping Report[391] and in Chapter 4 of this Consultation Paper, manifold categories of harm arising from online abuse: (1) emotional and psychological harms; (2) physiological harms, including suicide and

[391] Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381.

self-harm; (3) exclusion from public online space and corresponding feelings of isolation; (4) economic harms; and (5) wider societal harms. All of these harms form part of the justification for our proposed new offence. However, we do not think it is appropriate to build all of these harms into the offence itself. As we explain in Chapter 4, it seems consistently true of abusive online communications that they directly (rather than indirectly) cause, or are likely to cause, emotional or psychological harm to those who see, hear, or otherwise encounter them. This direct harm should be the basis of a new offence addressing online abuse.

5.96 Where other direct harms are caused by online abuse, our view is that these harms are or should be addressed by a better-targeted offence. For example, where a communication is sent or posted to cause physical harm deliberately and directly – such as flashing strobe lights sent or posted to cause an epileptic person to have a seizure, or an extremely loud noise sent to cause hearing damage – this may be better addressed as an offence against the person.[392] Or, as we have said above, where a communication is sent fraudulently, and causes economic harm, this may be better addressed by offences under the Fraud Act 2006.

5.97 The actual harms suffered by a victim – across all categories – could be taken into account at sentencing. However, building them into the proposed new offence would likely result in over-criminalisation: if we were to take this approach, the offence would risk covering conduct that is already criminalised under existing, and better-targeted, offences (such as fraud, for example); it may cover conduct where the harms are too indirect and remote to justify criminalisation; and the offence would be too broad for their application to be readily foreseeable by the defendant (and may therefore violate Articles 10 of the European Convention on Human Rights – see Chapter 2).

### The threshold of harm: "at least serious emotional distress"

5.98 In our proposal, the appropriate threshold of harm is emotional or psychological harm amounting to at least serious emotional distress. In this respect, the proposed new offence resembles the New Zealand model, where harm is defined as "serious emotional distress". However, our model differs in that the definition is broader: it includes other emotional and psychological harms, provided they are at least as serious as serious emotional distress.

5.99 In justifying the definition of "harm" as "serious emotional distress", the New Zealand Law Commission said:

> Not all harms arising from communications are proscribed by law. The criminal law has typically been concerned with protecting citizens from communication harms which invoke fear for physical consequences, either personal or proprietary, or which are obscene or harmful to children. The civil law, in the past, also typically shied away from protecting emotional harm as such. However, as we demonstrate later, in both civil and criminal spheres the law has been moving towards recognition and protection of that sort of harm. We recognise that within the community at large and within younger demographics particularly, the threshold for when a communication causes the level of distress that can be described as "harmful" and

[392] See our discussion in Chapter 4.

when it simply causes annoyance or irritation may sometimes raise difficult issues at the margins. But we have reached the view that when the level of emotional distress can be described as significant the law has a role to play.[393]

5.100 The New Zealand Law Commission considered whether proving that a communication had caused, or was likely to cause, serious emotional distress would prove too difficult. They thought that it would not:

> Proof of significant emotional distress may be thought to be problematic. Usually it will be sufficiently demonstrated by the nature of the communication itself: much of the material coming before the tribunal is likely to be of such a kind that it would clearly cause real distress to any reasonable person in the position of the applicant. This blended objective/subjective standard is reflected in the Harassment Act which requires, as a condition of making a restraining order, that the behaviour causes distress to the applicant, and is of such a kind that would it cause distress to a reasonable person in the applicant's particular circumstances. The Privacy Act requirement that an interference with privacy must cause damage including "significant humiliation, significant loss of dignity or significant injury to the feelings of the complainant" appears not to have been problematic.[394]

5.101 Under our model, no proof of actual emotional distress is required. The question is purely objective: was the communication likely to cause harm to someone likely to see, hear, or otherwise encounter it? However, many of the New Zealand Law Commission's observations are nonetheless relevant.

5.102 We agree that, when the level of emotional distress reaches a certain threshold, the criminal law has a role to play. Of course, other, comparable offences in the jurisdiction of England and Wales use different, and sometimes lower, thresholds of harm. For example, under the Protection from Harassment Act 1997 ("PHA 1997"), which we discuss in detail in Chapter 3, "harassing a person include[s] alarming the person or causing the person distress". The level of distress does not, under this offence, need to be "serious" for the threshold to be met. However, the offences under the PHA 1997 include additional elements that justify this lower threshold. First, the prosecution must show that the effect of the conduct was that the victim was actually harassed. Under our proposed offence, no actual harm is required. Second, the offences under the PHA 1997 require a course of conduct. Our proposed offence can be committed by sending a single communication. In our view, it is therefore appropriate that the threshold of harm under our proposed new offence should be higher.

5.103 Section 76 of the Serious Crime Act 2015 ("SCA 2015") criminalises controlling or coercive behaviour in an intimate or family relationship. The offence under section 76 requires that the defendant's conduct has "a serious effect on B [the victim]". Under section 76(4), the conduct has a "serious effect" if:

---

393 New Zealand Law Commission, *Ministerial Briefing Paper on Harmful Digital Communications: the adequacy of the current sanctions and remedies* (August 2012), at p 25.

394 New Zealand Law Commission, *Ministerial Briefing Paper on Harmful Digital Communications: the adequacy of the current sanctions and remedies* (August 2012), at p 113.

(a) it causes B to fear, on at least two occasions, that violence will be used against B, or

(b) it causes B serious alarm or distress which has a substantial adverse effect on B's usual day-to-day activities.

5.104 This offence is designed to address domestic abuse. Although it is, like our proposed offence, triable either-way, the maximum penalty on indictment is five years' imprisonment (as compared to two years' imprisonment for the existing communications offence under the MCA 1988). It is a more serious offence, and the harm threshold is correspondingly higher: not only must the victim be caused serious alarm or distress, there is an additional requirement that this has a substantial adverse effect on their day-to-day activities.

5.105 In short, our view is that "serious emotional distress" is an appropriate threshold of harm for our proposed new offence, taking account of other, comparable offences in England and Wales, as well as the offence under New Zealand's HDCA 2015.

5.106 In the case of *B v New Zealand Police*[395] the High Court of New Zealand considered the definition of harm as serious emotional distress. The High Court summarised the evidence of the complainant and of a witness, J, as follows:

> the complainant's unchallenged evidence was that she suffered considerable emotional distress. She said 'I was very upset for a long time; stressed ... it actually caused a lot of frustration, anger, I was anxious, medically I felt unfit to work for a few days because I was just, I was just really upset'. J's unchallenged evidence was to like effect. She said the complainant was 'very shocked' and 'very depressed'.[396]

5.107 The High Court held that the judge in the District Court erred in concluding that this evidence could not establish harm, that is, serious emotional distress. This was because "the Judge approached the issue by isolating the various descriptions of how the complainant felt, rather than—as required—assessing the evidence in its totality."[397]

5.108 In reaching this decision, the High Court made five observations:

(1) First, the definition is exhaustive. Consistently with its legislative history, the Act is concerned only with emotional harm, and more particularly, serious emotional distress.

(2) Second, and again consistently with its legislative history, the Act eschews minor emotional distress—indeed all distress falling short of that amounting to serious emotional distress. This reflects the criminal nature of the sanction (in s 22) and New Zealand's ongoing commitment to freedom of expression, as affirmed by s 14 of the Bill of Rights Act. However… the Act does not equate harm with mental injury, nor insist upon the establishment of an identifiable

---

395 [2017] NZHC 526

396 *B v New Zealand Police* [2017] NZHC 526, [2017] 3 NZLR 203 at [36].

397 *B v New Zealand Police* [2017] NZHC 526, [2017] 3 NZLR 203 at [35].

psychological or psychiatric condition. The offence is complete when the defendant causes the complainant serious emotional distress.

(3) Third, that determination is part fact, part value-judgment. The Law Commission appears to have recognised as much. So too the legislature given its adoption of a somewhat elastic concept, and its articulation of permissive factors in the context of whether the post would cause harm to an ordinary reasonable person in the position of the complainant.

(4) Fourth, in determining whether serious emotional distress has been caused… consideration should be given to obvious factors such as the nature of the emotional distress; its intensity; duration; manifestation; and context, including whether a reasonable person in the complainant's position would have suffered serious emotional distress.

(5) Fifth, doubt attaches to whether interpretation or application of the phrase "serious emotional distress" is much helped by reference to a dictionary or thesaurus. I have avoided both for this reason. As the Court of Appeal observed in *Stockco Ltd v Gibson*:[398]

> ... we doubt that much is to be gained by using synonyms of statutory language. In the end the statutory words ["ordinary course of business of the seller"] are everyday terms having common meaning and are reasonably clear in their own right. The hard part is applying them to the facts of the case. We do not think that the exercise is greatly assisted by applying the facts to similar but not identical wording.[399]

5.109 For our purposes, the first of these points is not relevant: the definition is not exhaustive. Rather, it sets a threshold – any emotional or psychological harm must be at least as serious as serious emotional distress. This is because we do not want to rule out communications likely to cause serious emotional or psychological harm of a kind that may not accurately be described as "distress", such as, for example, post-traumatic stress disorder or body dysmorphia. While "serious emotional distress" sets a floor, or threshold, below which the level of likely harm cannot fall if it is to come within the scope of the proposed offence, "emotional and psychological" serves as a boundary, delineating the categories of harm with which the offence is concerned.

5.110 The second and fourth points are, in our view, perhaps the most helpful in the context of our proposed offence. Regarding the second point, our proposed offence would not address minor emotional distress – this threshold reflects the criminal nature of the sanction and protects freedom of expression – but nor does it require the prosecution to establish that the communication was likely to cause a medically recognised psychiatric condition. "Serious emotional distress" lies between minor emotional distress and a medical condition. That being said, by "serious" we do not simply mean anything more than minor. Rather, we mean a big, sizable harm.

---

398 *Stockco Ltd v Gibson* [2012] NZCA 330.

399 *B v New Zealand Police* [2017] NZHC 526, [2017] 3 NZLR 203 at [21] - [25].

5.111 Regarding the fourth point, in determining the threshold of "serious emotional distress" relevant factors will include the nature of the emotional distress; its intensity; duration; and manifestation. For example, several days of intense distress, with "manifestations" such as sleeplessness, reduced appetite, or crying spells would likely meet the threshold. While such physical manifestations are not necessary for the threshold to be met – the test is about *likely* harm, rather than actual harm – they are indicative of what is meant by serious emotional distress. Further, some impact on daily life, such as avoiding a platform where the abuse took place, cancelling social engagements, or reduced productivity at work, would be indicative that the level of emotional distress might be sufficiently "serious". As we indicate above at 1.104, we do not propose to mirror the approach under section 76 SCA 2015 and *require* that the communication was likely to have a *substantial* adverse effect on daily life *as well as* being likely to cause serious emotional distress. However, some impact on daily life is another "manifestation" indicating serious emotional distress.[400]

5.112 While we recognise that there may be some cases where the distinction between emotional distress and serious emotional distress is somewhat fine, we do not think that this poses an insurmountable difficulty. Our view on this matter was formed partly in light of pre-consultation meetings with the Magistrates' Association, and in light of other, existing offences that require courts and law enforcement agencies to make distinctions on the basis of "seriousness" of harm; including the aforementioned offence under the SCA 2015, and the offences in the Offences Against the Person Act 1861 discussed in Chapter 4.

5.113 Finally, it bears repeating that the proposed offence does not require proof of actual harm. In many cases, the nature of the communication will be sufficient to demonstrate that it was likely to cause serious emotional distress – though there will be other occasions where the harmfulness of the communication will not be evident on its face. Instead, this will be apparent only in light of contextual factors, such as a history of domestic abuse or the fact that the communication was sent as part of a pile-on (see Chapter 4).

5.114 Having said this, we acknowledge that it may be helpful for the proposed offence to include additional guidance as to the threshold set by the term "serious emotional distress". One approach would be to include some of the factors from the New Zealand jurisprudence – such as intensity, duration, and manifestation – in the offence itself, to indicate what is meant by "serious emotional distress". A drawback of this approach might be that it risks giving the false impression that proof of actual harm is required. We would welcome consultees' views on whether such a list of factors should be included in the offence.

---

400 We depart from the New Zealand approach in the following respect: whether a reasonable person in the complainant's position would have suffered serious emotional distress does not have any role in our proposed offence. For further discussion of this point, see below at 1.131-1.134.

**Consultation Question 5.**

5.115 "Harm" for the purposes of the offence should be defined as emotional or psychological harm, amounting to at least serious emotional distress. Do consultees agree?

5.116 If consultees agree that "harm" should be defined as emotional or psychological harm, amounting to at least serious emotional distress, should the offence include a list of factors to indicate what is meant by "serious emotional distress"?

### Requirement to consider "the context in which the communication was sent or posted, including the characteristics of a likely audience"

5.117 The proposed new offence specifies that, in determining whether the communication was likely to cause harm, the court must have regard to the context in which the communication was sent or posted, including the characteristics of a likely audience.

5.118 This can be contrasted with the list of factors that appears as part of the New Zealand model, which includes:

(a) the extremity of the language used;

(b) the age and characteristics of the victim;

(c) whether the digital communication was anonymous;

(d) whether the digital communication was repeated;

(e) the extent of circulation of the digital communication;

(f) whether the digital communication is true or false;

(g) the context in which the digital communication appeared.

5.119 We consider that there are disadvantages in including a list of factors. Reasons that count against including such a list is that it may direct attention away from the pertinent features of a given case, if such features are not covered by the list. In addition, these factors may not always point in one direction. For example, a false message could be more harmful, because it spreads misinformation on which people may rely, or less, because it doesn't reveal a damaging truth. It may, therefore, be better to leave it to the court to make a judgement about the factors contributing to the likelihood of harm on a case-by-case basis.

5.120 Despite the disadvantages of including a full list of factors, our provisional view is that the offence should specify that likely harm should be assessed in light of the context, including the characteristics of the likely audience. A consistent message from stakeholders has been that, often, the harmful nature of a communication is not evident solely on its face. Instead, we recognise that context is often key to understanding how and why a communication is harmful. This is also consistent with

the approach to the existing communications offences taken by the CPS in their *Guidelines on prosecuting cases involving communications sent via social media*. As we explain in Chapters 2 and 3, these guidelines state:

> 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?[401]

5.121 The requirement that the court must have regard to the characteristics of a likely audience helps to ensure that the proposed offence would adequately address online hate. In our Hate Crime Report (2014), the Law Commission noted that "a sharp rise in internet and social media based hate crime has been reported including extremist and anti-Muslim content."[402] Therefore, "there may be an argument for aggravated forms of some of the communication offences."[403] Our provisional view is that the proposed offence may be a suitable candidate for inclusion in the list of aggravated offences under hate crime legislation. This is because a subset of communications likely to cause serious emotional distress, taking account of the context in which the communication was sent or posted, including the characteristics of a likely audience, are also likely to involve hostility towards people with characteristics protected under hate crime legislation.[404] The possibility of including communications offences (whether the existing communications offences or our proposed offence) is considered as part of the Law Commission's separate Consultation Paper on hate crime.[405]

5.122 We note that it may sometimes be the case that the aggravating factor – such as the use of racial slurs – is also part of the offence itself: the use of a racial slur may push a communication over the line of criminality in the first place, as well as aggravating the offence. This may seem to pose a risk of "double counting" (that is, that the defendant will be punished twice for the same feature of the case). However, we think this problem can be avoided.

5.123 The usual approach (set out in *R v Kelly*)[406] is to decide what the sentence would otherwise have been and then increase the sentence to take account of the aggravating factor. However, where the aggravating factor is part of the offence itself, the courts have adapted their approach accordingly. In *R v Fitzgerald*, it was

---

401 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media* (last revised 21 August 2018), https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (last visited 09 September 2020).

402 Hate Crime: Should the current offences be extended? (2014) Law Com No 348 at 5.31.

403 Hate Crime: Should the current offences be extended? (2014) Law Com No 348 at 5.31.

404 We note that, as part of our work on hate crime, we are consulting on expanding the test to include prejudicial targeting as well as demonstrated hostility. The Law Commission's Consultation Paper on hate crime is available at www.lawcom.gov.uk.

405 The Law Commission's Consultation Paper on hate crime is available at www.lawcom.gov.uk.

406 [2001] EWCA Crim 170, [2001] Crim. L.R. 411.

acknowledged that, in some cases, "the racial aggravation of the offence is so inherent and integral to the offence itself that it is not possible sensibly to assess the overall criminality involved in such a discrete way. In such cases, the Court must assess the seriousness of the conduct involved and its criminality as a whole."[407] This approach avoids the potential issue of "double counting". Hence, in our provisional view, the proposed offence may be suitable for inclusion in the aggravated offences regime, even if the aggravating factor is sometimes part of the offence itself.

**Example 2: online hate**

Xavier writes a Tweet directed at a well-known disability charity with around 100,000 Twitter followers. He uses the '@' function to ensure that the Tweets will come to the attention of the administrators and followers of the charity's Twitter page.

He writes: "Stop scrounging off the state, you loser scum. Let's face it, we'd all be better off without your disgusting, deformed bodies fouling up the place. Evolution will destroy you eventually. Can't fucking wait."

5.124 A court should find that Xavier's Tweet would be likely to cause harm to a likely audience. This should be especially easy to show since the likely audience was, primarily, the disability charity and its followers (many of whom will, we can assume, have a disability): clearly, a disabled person would be especially likely be caused at least serious emotional distress by the content of the Tweet. Moreover, Xavier would likely have been aware of a risk of harm. Given that the charity has a fairly large Twitter following, the prosecution may well be able to prove that Xavier was aware of a risk that at least one of the followers would be caused serious emotional distress. Finally, it is highly unlikely that Xavier could show that he had a reasonable excuse.

5.125 Hence, Xavier's conduct would likely be caught by the proposed new offence. The ableist nature of the Tweet may also mean that it would be caught under an aggravated form of the offence and, therefore, be a hate crime.

5.126 It is important to note, however, that we do not intend "characteristics" in this context to be limited to protected characteristics for the purposes of hate crime legislation. "Characteristics" could include, for example, age, gender, or social class. These are not currently protected characteristics under hate crime legislation[408] but, regardless, they could be relevant for the purposes of our proposed offence.

5.127 Under our proposed communications offence, the question is: taking account of contextual factors, including the fact that the person likely to encounter the

---

[407] *R v Fitzgerald* [2003] EWCA Crim 2875, at [11]. See also *R v Bailey* [2011] EWCA Crim 1979: racist comments were spray painted onto a vehicle: this was not criminal damage plus an element of racial aggravation – it was racist abuse committed by way of criminal damage, and a two-stage approach would be inappropriate.

[408] We note, however, that in the Law Commission's separate Consultation Paper on hate crime, we make a provisional proposal to include gender as a protected characteristic. The Law Commission's Consultation Paper on hate crime is available at www.lawcom.gov.uk.

communication was, for example, a young girl with special educational needs, was the communication likely to cause harm to this person? Or, taking account of contextual factors, including the fact that the person likely to encounter the communication was a retired working-class man, was the communication likely to cause harm to this person?

5.128 It should be noted that the contextual factors and characteristics of a likely audience have the potential to decrease, as well as increase, the likelihood that the communication would cause harm. As we explain in more detail below, at 1.191-1.198, a joke in very bad taste between friends would not be caught by the proposed offence if it was not likely to cause harm, given the disposition of the likely audience (the likely audience being the person who shares their friend's sense of humour).

5.129 The fact that a given characteristic is relevant when considering whether a communication was likely to cause harm does not automatically mean that the characteristic should be protected under hate crime legislation. In our consultation on hate crime, we provisionally propose criteria for deciding whether any additional characteristics should be recognised in hate crime laws.

**Consultation Question 6.**

5.130 We provisionally propose that the offence should specify that, when considering whether the communication was likely to cause harm, the court must have regard to the context in which the communication was sent or posted, including the characteristics of a likely audience. Do consultees agree?

### Particular sensitivities of a likely audience

5.131 The current formulation – "the defendant sent or posted a communication that was likely to cause harm to a likely audience" – means that the defendant could be liable even if, on objective analysis of the facts, the likely audience was unusually sensitive or prone to serious emotional distress. Absent the fault element, this might be seen to place an unfair burden on the defendant: they sent or posted out a message that would have caused no harm to the majority of people, yet they risk being prosecuted because it is determined that those likely to see, hear, or otherwise encounter the communication happened to include people who were unusually sensitive to the content. This gives rise to the following question: should the "likely harm" test be subject to a reasonableness requirement, such that the defendant would be guilty only if the communication would likely cause harm to the reasonable person (that is, the person of normal disposition and fortitude)? We are of the view that, given the proposed mental elements in our model offence, such a requirement would not be appropriate.

5.132 If the defendant intended to cause harm, the defendant should be culpable even if the likely audience was exceptionally vulnerable. Indeed, if the defendant intended to cause harm, it may be that they deliberately exploited the audience's vulnerability. Either way, the intention creates a relationship of proximity between the defendant and the victim: the defendant is to take the victim as they find them, not as they might

conveniently wish them to have been after the event. In such circumstances, the defendant should not be able to escape liability by arguing that, whilst they intended harm, the majority of people would not have suffered harm.

5.133 Similarly, where the defendant did not specifically intend harm but was nonetheless aware of the risk of harm, there seems little merit in limiting the scope of their liability by requiring that their actions would only harm those of ordinary fortitude and sensitivity. So long as the defendant is aware of the risk of harm, why should it matter that harm was in fact far more likely than they had appreciated owing to the sensitivity of those likely to be exposed to the communication? Given the limitation that these fault elements place on the scope of the offence, we cannot see a justification for imposing further limits by references to the "reasonable person", "person of ordinary fortitude" or other similar factors.

5.134 It is further worth recalling that the offence is complete only if it is established that the defendant lacked a reasonable excuse in sending the communication. To the extent that any injustice may be suffered as a result of "likely harm" not being subject to a reasonableness requirement – which we doubt – the defendant will have the opportunity to introduce evidence that their communication was nonetheless sent or posted with reasonable excuse.

**Consultation Question 7.**

5.135 We provisionally propose that the new offence should not include a requirement that the communication was likely to cause harm *to a reasonable person* in the position of a likely audience. Do consultees agree?

## THE MENTAL AND FAULT ELEMENTS

5.136 The mental element of the proposed offence is that the defendant intended to harm, or was aware of a risk of harming, a likely audience. The offence also includes a requirement that the defendant sent or posted the communication without reasonable excuse.

### "Intended or was aware of a risk of harm"

5.137 Under the proposed new offence, there are two, alternative mental elements. The first is intention to cause harm to a likely audience and the second is awareness of a risk of harm to a likely audience (where "harm" is defined as emotional or psychological harm amounting to at least serious emotional distress and a "likely audience" is someone who, at the time the communication was sent or posted by the defendant, was likely to see, hear, or otherwise encounter it).

5.138 This distinguishes the proposed new offence from section 22 HDCA 2015, section 1 MCA 1988, and section 127 CA 2003. Under the section 22 HDCA 2015 offence and the section 1 MCA 1988 offence, the mental element is intention. Under the section 127 offence, there is no express provision for the mental element, but in the case law

(*Collins*[409] and *Chambers*[410]), it has been held that the defendant must intend to send a message of the proscribed character (if, for example, the defendant sent a menacing message, he or she must have intended that it would be menacing).

5.139 As we mentioned above, given the considerations set out in the Criminal Gateway Guidance regarding the appropriate role of the criminal law, it is important that harmful but non-culpable behaviour is not caught by the proposed new offence. The mental element of the proposed new offence helps to ensure that this is the case.

5.140 The purpose of having the two, alternative mental elements is to criminalise appropriately the various types of abusive communications: some abusive communications should be criminal, even though there is no intention to cause harm. To see this, consider the following example:

**Example 3: awareness of a risk of harm**

Toby and Jacob are work colleagues and Facebook "friends". They do not know each other very well, but Toby does know that Jacob is Jewish and celebrates Hanukkah.

On Hanukkah, Toby posts a photoshopped image on Jacob's Facebook wall. The background of the image is a photograph from the early 1940s, depicting Jewish people interned at Auschwitz concentration camp. Toby has edited the image so that Jacob, his wife, and their young children appear to be among the people interned in the camp.

The accompanying messages reads "Happy Hanukkah, mate! Have a good one." Toby intends that Jacob will find this funny.

5.141 In our view, Toby's post is, at least arguably, worthy of criminalisation. However, if the mental element were restricted to intention to cause harm, then Toby's post – and other, comparable communications – would not be caught by our proposed new offence.

5.142 That a defendant can be criminally liable where they did not intend but were merely aware of a risk of harm has a strong basis in legal theory. For example, writing about the justifications for recklessness in the criminal law, Professor Glanville Williams said:

> We learn as a result of experience and instruction, and our learning brings awareness of the dangers of life. We can guess at the probable present even when

409 *DPP v Collins* [2006] UKHL 40, [2006] 1 WLR 2223 at [11].

410 *Chambers v DPP* [2012] EWHC 2157 (Admin), [2013] 1 WLR 1833 at [38].

> we cannot directly perceive it, and can project ourselves into the future by foreseeing the probable consequences of our acts.[411]

5.143 As Glanville Williams noted, even before recklessness was regularly used in statutes as an explicit alternative to intention, it was incorporated into the notion of intention through the use of various judicial techniques. For example, citing Lord Hailsham in *DPP v Morgan*,[412] Glanville Williams observed:

> The presumption about intending probable consequences was used to make the notion of intention cover what we now term recklessness (and it covered negligence as well).[413]

5.144 In short, mental elements falling short of intention (narrowly defined) have long been recognised as sufficient for criminal culpability.

5.145 Other examples of criminally culpable communications where the defendant did not intend, but was aware of a risk of harm may include some instances of cyberflashing. Case studies, including those collected by journalist Moya Sarner, suggest that some perpetrators act for their own sexual gratification or for a sense of validation.[414] They may be aware of a risk of harm, but – arguably – causing harm is not their intention. (We discuss cyberflashing further in Chapter 6.)

5.146 Alternatively, in such cases, the defendant may intend to cause harm, but proving that this is the case would be too onerous: the defendant could argue that they thought receiving an unsolicited picture of their genitals would be flattering, pleasurable, or otherwise welcome, and in the face of such arguments the prosecution would have to prove beyond reasonable doubt that the defendant intended to cause harm. Restricting the mental element to intention may, then, prevent successful prosecution of criminally culpable communications.

5.147 Our provisional view is that including subjective awareness of a risk of harm, as an alternative to intention to cause harm, is necessary if the offence is adequately to address abusive online communications. Where there is intention to cause harm, there may be a higher degree of culpability and this should be reflected at sentencing.

**Consultation Question 8.**

5.148 We provisionally propose that the mental element of the offence should include subjective awareness of a risk of harm, as well as intention to cause harm. Do consultees agree?

---

411 D J Baker, Glanville Williams Textbook of the Criminal Law (4th ed 2015), at p 127.

412 *DPP v Morgan* [1976] AC 182 at 230, 209, 225.

413 D J Baker, Glanville Williams Textbook of the Criminal Law (4th ed, 2015), at p 128.

414 M Sarner, *What makes men send dick pics?* (08 January 2019), https://www.theguardian.com/society/2019/jan/08/what-makes-men-send-dick-pics (last visited 09 September 2020).

5.149 Instead of awareness of a *risk* of harm, another option would be to frame the mental element in terms of awareness of a *likelihood* of harm. This would correspond to the conduct element, which is that the defendant sent or posted a communication *likely* to cause harm (to someone likely to see, hear, or otherwise encounter it). The question would then be: was the defendant aware that the communication was likely to cause harm to a likely audience?

5.150 However, there is no principle of criminal law that requires the mental and conduct elements to match in this way.

5.151 Further, while it should be relatively easy to prove that Toby (in the example above) was aware that his Holocaust "joke" posed a *risk* of harm to Jacob (who was the likely audience of the communication), it would be less easy to prove that he was aware that it was *likely* to cause harm to Jacob. On its own, of course, this reason is unpersuasive: if the criminal culpability should only attach to the higher threshold (awareness of likely harm), then making it more difficult to prove this element would be justifiable. However, as we have noted above, there is moral culpability in taking unreasonable risk (which is to say, risk without reasonable excuse). This is a similar formulation to recklessness, and "nearly all crimes requiring *mens rea* [mental fault] recognise recklessness as an alternative to intention."[415] Therefore, making it more difficult to prosecute Toby's conduct is not justified.

5.152 Hence, our provisional view as we provisionally propose above at 1.147 is that the mental element should be framed in terms of awareness of a risk of harm, rather than likelihood of harm. We would, however, welcome consultees' views on this point.

**Consultation Question 9.**

5.153 Rather than awareness of a *risk* of harm, should the mental element instead include awareness of a *likelihood* of harm?

5.154 We note that the offences under the PHA 1997 and section 76 of the SCA 2015 have objective knowledge tests: they require that the defendant "knows or ought to have known" the relevant matter (in the case of the PHA 1997, the relevant matter is that their conduct amounts to harassment; in the case of section 76 of the SCA 2015, it is that their behaviour will have a serious effect on the victim).

5.155 In our view, an objective knowledge test would not be appropriate given the other elements of our proposed new offence: unlike the offences under the PHA 1997, the conduct element can be met even if the defendant sends a one-off communication; unlike either the PHA 1997 or section 76 of the SCA 2015, no actual harm is required. If our proposed new communications offence included an objective knowledge test, the offence could be too easily made out.

5.156 An alternative way to include subjective awareness of a risk of harm would be to have two different offences: one offence with a mental element of intention to cause to

[415] D J Baker, Glanville Williams Textbook of the Criminal Law (4th edition, 2015), at para 5-001.

harm; and one offence with a mental element of awareness of a risk of causing harm. The first offence could be triable either-way, and the second offence could be summary-only.

5.157 One advantage of this approach is that it would reduce the number of Crown Court trials in relation to relatively low-level offences, where harm was not necessarily caused nor was it intended. Where the defendant did not intend, but was merely aware of a risk of causing harm, the offence would automatically be tried in the Magistrates' court. If there is only one, either-way offence, there is a risk that the vast majority of defendants will elect trial by jury in the Crown Court, placing a heavier burden on the criminal justice system. We are conscious that this is a particular concern in the wake of the COVID-19 pandemic, given the backlog of cases to which it has given rise.

5.158 That being said, we have concerns about the two-offence approach. First, it is not clear that conduct involving awareness of a risk of harm, as opposed to intention, consistently warrants a summary-only rather than an either-way offence. Consider, for example, those instances of cyber-flashing where the defendant did not necessarily intend but was aware of a risk of harm, and the Holocaust "joke" example (above, at 1.140. Second, we have not been able to find other offences constructed in this way, where there is a summary-only offence with a fault element of recklessness, and a corresponding either-way offence with a fault element of intention. Finally, such an approach would likely lead to difficult charging decisions: if there are any obstacles to proving intention, the CPS may feel compelled to charge the lesser, summary-only offence, even if the perpetrator's conduct is egregious.

5.159 Given that there are significant advantages and disadvantages of the two-offence approach, we would welcome consultees' views on this issue.

**Consultation Question 10.**

5.160 Assuming that there would, in either case, be an additional requirement that the defendant sent or posted the communication without reasonable excuse, should there be:

(1) one offence with two, alternative mental elements (intention to cause harm or awareness of a risk of causing harm); or

(2) two offences, one with a mental element of intention to cause harm, which would be triable either-way, and one with a mental element of awareness of a risk of causing harm, which would be a summary only offence?

### "Without reasonable excuse"

5.161 We propose that the offence should include a requirement that the communication was sent or posted without reasonable excuse. This is not a defence. Rather, it is part of the offence itself. The burden would be on the prosecution to prove that the communication was sent or posted *without* reasonable excuse. It should not be for the

defence to prove that the communication was sent or posted *with* reasonable excuse.[416]

5.162 This is consistent with case law on "reasonable excuse" in the context of, for example, section 1(10) Crime and Disorder Act 1998. Section 1(10) provides that "If without reasonable excuse a person does anything which he is prohibited from doing by an Anti Social Behaviour Order, he is guilty of an offence." In the case of *R v Charles*,[417] the Court of Appeal held that it was for the prosecution to prove that there was no reasonable excuse for doing what was prohibited by the order, and that this had to be done to the criminal standard of proof (that is, beyond reasonable doubt).[418] Under the proposed new offence, the burden would likewise be on the prosecution.

5.163 Where the defendant did not intend but was aware of a risk of harm, there is a particularly strong need for a "defence" of reasonableness. There are many communications of such kind that a defendant would, in most cases, foresee a risk of causing serious emotional distress. But these communications may nonetheless be legitimate. One significant category could broadly be described as "delivering bad news". This might include:

- telling someone that they are bereaved or that they have a terminal illness;
- informing a romantic partner of a desire to end the relationship; and
- sending a formal communication regarding a change in legal status, such as a refusal of a housing, social security payment, or immigration application.

5.164 In all of these cases, a defendant is likely to be aware of a risk of causing serious emotional distress. But it is clear that such communications should not, without more, be criminal. This explains the need for a requirement that the communication is sent or posted without reasonable excuse. Indeed, we consider this requirement to be crucial in order to ensure that the proposed offence is not overly broad and that the right to freedom of expression is protected. We discuss the relationship between Article 10 ECHR and the "without reasonable excuse" requirement below at 1.168-1.169.

5.165 "Reasonable excuse" does not have any precise definition. In the case of *R v AY*,[419] the Court of Appeal held that "The concept of 'reasonable excuse' is par excellence a concept for decision by the jury on the individual facts of each case."[420] In *R v G*,[421]

---

416 Albeit that the evidential burden would be on the defendant. This means that the defendant would be required to produce evidence that they had a reasonable excuse, but it would be for the prosecution to prove beyond reasonable doubt that they did not.

417 *R v Charles* [2009] EWCA Crim 1570.

418 In so doing, the Court of Appeal affirmed the position Judicial Studies Board Guide, which itself relied on the decision in *R v Evans* [2004] EWCA Crim 3102*,* regarding an analogous provision; section 5(5) of the Protection from Harassment Act 1997.

419 *R v AY* [2010] EWCA Crim 762.

420 *R v AY* [2010] EWCA Crim 762 at [25].

421 *R v G* [2009] UKHL 13.

Lord Rodger observed that "It is comparatively easy to identify examples of excuses which could never be regarded as reasonable. It is similarly easy to give examples of excuses which everyone would regard as reasonable".[422] However, there is also a "middle range" of cases, which must be left to the jury.[423]

5.166 The case of *JB v DPP*[424] helpfully enumerates the various contexts in which the defence of reasonable excuse appears. These include: section 7(6) of the Road Traffic Act 1988; section 9 (1) of the Prevention of Terrorism Act 2005; section 113 of the Sexual Offences Act 2003; section 5(5) of the Protection from Harassment Act 1997; section 42A (1) of the Domestic Violence, Crime and Victims Act 2004; section 80(4) and (6) the Environmental Protection Act; section 6(1) of the Bail Act 1976; and section 14J of the Football Spectators Act 1989.[425] We can now add to this list the Health Protection (Coronavirus, Restrictions) (England) Regulations 2020. Naturally, the application of the defence will depend on the context. Lord Rodger in his judgment in *R v G* compared reasonable excuse in the context of refusing to give a sample of blood or urine to reasonable excuse in the context of carrying an offensive weapon in a public place:

> the Court of Appeal had indicated that only a very narrow range of circumstances could amount to a reasonable excuse for refusing to give a sample of blood or urine. But that approach is only possible because the circumstances giving rise to the offence are always essentially similar and so it is possible to envisage what could be a reasonable excuse for doing what it prohibits. By contrast, under the Prevention of Crime Act 1953 and the Criminal Law (Consolidation) (Scotland) Act 1995 the circumstances in which people may have an offensive weapon in a public place are many and various. So the courts have recognised that any decision on whether an accused had a reasonable excuse must depend on the particular circumstances of the case. For example, a male stripper dressed as a police officer, who was waiting outside for his performance to begin, was held to have a reasonable excuse for carrying a truncheon in a public place: Frame v Kennedy 2008 SCCR 382. Similarly, the circumstances which may give rise to a section 58(1) offence are many and various. So it is impossible to envisage everything that could amount to a reasonable excuse for doing what it prohibits. Ultimately, in this middle range of cases, whether or not an excuse is reasonable has to be determined in the light of the particular facts and circumstances of the individual case. Unless the judge is satisfied that no reasonable jury could regard the defendant's excuse as reasonable, the judge must leave the matter for the jury to decide.[426]

5.167 In our view, the flexibility of the concept makes it well-suited to the context of abusive communications. Given the nature of communication, it is very difficult – impossible even – to set out in advance the complete set of situations in which a communication should not be criminal, despite meeting the other elements of the proposed new offence. While the open-endedness of what might constitute a reasonable excuse

---

422 *R v G* [2009] UKHL 13 at [81].

423 *R v G* [2009] UKHL 13 at [81].

424 *JB v DPP* [2012] EWHC 72.

425 *JB v DPP* [2012] EWHC 72 at [14].

426 *R v G* [2009] UKHL 13 at [81].

introduces some uncertainty, by specifying factors that the court must consider when deciding whether the defendant had a reasonable excuse, we mitigate the risk that the concept will be interpreted in an overly narrow way. At the same time, it is open to the court to find that the defendant had a reasonable excuse on the basis of factors other than those specified in the statute.

5.168 Further, under section 3 of the Human Rights Act 1988, the courts have an obligation to interpret primary legislation in a way which is compatible with the Convention rights: reasonableness would, therefore, need to be interpreted in a way compatible with Article 10 of the European Convention on Human Rights ("ECHR").[427] In our view, then, the proposed new offence affords better protection to freedom of expression than the existing communications offences, despite the vagueness inherent in the concept of "reasonable excuse".

5.169 In this regard, we also note that Joint Committee on Human Rights in their report on the Terrorism Bill (which later became the Terrorism Act 2006), recommended that a "reasonable excuse" or "public interest" defence should be included in the encouragement of terrorism offences (along with requirements of intent and likelihood). Their reasoning was that this would "make it less likely that the offence would be incompatible with Article 10 of the European Convention on Human Rights".[428]

### Recklessness as an alternative?

5.170 An alternative would be to formulate the mental and fault element in terms of "recklessness". At least until the case of *R v G,*[429] the case law regarding the interpretation of "recklessness" was mixed: there were two different standards for recklessness and it was not always clear which standard would apply. However, since the cases of *G,*[430] *Brady,*[431] and *Attorney General's Reference (No. 3 of 2003)*,[432] it seems that the *Cunningham*[433] standard for recklessness will apply across all offences. The defendant is reckless if: (1) they are subjectively aware of a risk of particular consequences or circumstances; and (2) it is, in the circumstances known to them, unreasonable to take that risk.

5.171 According to *Clarkson & Keating Criminal Law: Text and Materials*, "the test involves a subtle balancing operation between the following questions: how socially useful is the activity? What are the perceived chances of the harm occurring? How serious is the

---

427 Human Rights Act 1998, s 3. *Percy v DPP* [2001] EWHC Admin 1125, [2002] *Criminal Law Review* 835; discussed S Bailey and N Taylor, *Bailey, Harris and Jones: Civil Liberties, Cases, Materials & Commentary* (6th ed 2009) pp 348 to 350. For further discussion of Article 10 of the European Convention on Human Rights, see Chapter 2.

428 Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters, Report of the Joint Committee on Human Rights (2005-6) HL Paper 75-I, HC 561-I.

429 *R v G* [2003] UKHL 50, [2003] 3 W.L.R. 1060.

430 *R v G* [2003] UKHL 50, [2003] 3 W.L.R. 1060.

431 *R v Brady* [2006] EWCA Crim 2413; [2007] Crim. L.R. 564.

432 *Attorney General's Reference (No.3 of 2003)* [2004] EWCA Crim 868; [2005] Q.B. 73.

433 *R v Cunningham* [1957] 2 Q.B. 396; [1957] 3 W.L.R. 76.

harm that could occur?"[434] Drawing on the Law Commission's Working Paper on the mental element in crime,[435] the authors contrast the operation of high speed trains (with a subjectively perceived one in a thousand risk of death) with a game of Russian roulette (with the same subjectively perceived one in a thousand risk of death). In the case of the former, the decision to take the risk would be reasonable, given the social value of the activity. In the case of the latter, it would not.

5.172 Applying this reasoning to potentially harmful communications, in all of the examples given above at 1.163 – telling someone about a bereavement or illness; ending a romantic relationship; or communicating a change in legal status – a court would almost certainly find that the decision to take the risk was not unreasonable and that the defendant was not, therefore, reckless.

5.173 The requirements of our proposed new offence – awareness of a risk of harm, plus a requirement that the communication was sent or posted without reasonable excuse – should, in our view, produce the same results. There are, however, two main advantages of the proposed new offence as we have formulated it:

(1) First, it is possible that the common law test for recklessness may change. In an analogous situation, when the Fraud Act 2006 was passed (following Law Commission recommendations), "dishonesty" was determined by the *Ghosh*[436] test. This has since been replaced by the *Ivey*[437] test – as affirmed by *Barton and Booth.*[438] This may change substantially the effect of the Fraud Act. Our formulation of the proposed new offence mitigates against this kind of risk.

(2) Second, the proposed new offence is an either-way offence that may often be tried in the magistrates' courts. Where the offending is relatively low-level it is, in our view, appropriate that the offence should be as simple as possible. Under our formulation of the proposed new offence, all the main elements appear on its face, without the need to refer to case law.

5.174 Another option would be give a statutory definition of recklessness. However, as we explain below, we think that the "without reasonable excuse" requirement should also apply where the mental element is intention. Our formulation is intended to be as clear and straightforward as possible, making plain that the defendant must have acted without reasonable excuse, regardless of whether the mental element was intention or awareness of a risk.

---

434 S Kyd, T Elliott, and M A Walters, *Clarkson & Keating Criminal Law: Text and Materials* (2017) 2.189. See also *R v Dodman* [1998] 2 Cr. App. R. 338.

435 Codification of the Criminal Law, General Principles: The Mental Element in Crime (1970) Law Com No 31, at p 53.

436 *R v Ghosh* [1982] EWCA Crim 2, [1982] QB 1053.

437 *Ivey v Genting Casinos* [2017] UKSC 67, [2017] 3 WLR 1212.

438 *R v Barton and Booth* [2020] EWCA Crim 575.

### Should the defence of "reasonable excuse" apply where the mental element is intention?

5.175 The reasoning behind our view that the "without reasonable excuse" requirement should apply where the mental element is intention is illuminated most clearly by reference to examples. Consider the following:

> **Example 4: intention to cause harm but no criminal culpability**
>
> Alice and Thomas are the parents of a drug-dependent child, Celeste. They are increasingly concerned about their daughter's welfare. They paid for Celeste to attend a drug rehabilitation facility and they have taken various other measures to try and support her recovery. This has been to no avail.
>
> In a final attempt to help her, Alice and Thomas send Celeste a long email explaining their fears that she will die, and the sorrow it will cause them. They attach images and videos of families who have been similarly affected, in order to emphasise their point. They refer to Celeste's friend, who died of a drug overdose.
>
> In short, it is their intention to cause her serious emotional distress. This will, they hope, provide the impetus for her to finally stop using drugs.

5.176 In our view, the conduct in this example should not be criminal. This is because the conduct, though harmful, is not necessarily wrong. The example illustrates that, sometimes, there may be valid reasons for intentionally causing serious emotional distress through the communications that one sends. In order to avoid replicating the problem of over-criminalisation, our view is that the proposed new offence should avoid catching such conduct.

5.177 It may be tempting to think we can solve this problem by using "purpose" or "aim and objective" as the mental element, instead of intention. However, this would create more problems than it solves. It might allow a bully, who sends vile abuse to a victim, to mount a defence along the lines of, "It wasn't my aim and objective to upset him; I just wanted to impress my friends." It might allow a domestic abuser to mount a defence along the line of, "My purpose wasn't to upset her. I love her! My purpose was to make sure she didn't leave me."

5.178 In our view, the better way to avoid over-criminalisation is to include a requirement that the defendant sends the communication without reasonable excuse, even where the mental element is intention.

> **Consultation Question 11.**
>
> 5.179 We provisionally propose that the offence should include a requirement that the communication was sent or posted without reasonable excuse, applying both where the mental element is intention to cause harm and where the mental element is awareness of a risk of harm. Do consultees agree?

### "Was or was meant as a contribution to a matter of public interest"

5.180 The proposed offence includes a provision that, when deciding whether the defendant had a reasonable excuse for sending the communication, the court must have regard to whether the communication was or was meant as a contribution to a matter of public interest.

5.181 If a communication is or is meant as a contribution to a matter of public interest, then sending that communication – even if it is likely to cause harm – is much more likely to be reasonable. Therefore, on one view, the explicit protection afforded by this provision may be unnecessary because, if the communication is or is meant as a contribution to a matter of public interest, this would likely constitute a reasonable excuse regardless.

5.182 Nevertheless, we have included the provision to avoid the risk of disproportionately interfering with the right to freedom of expression under Article 10 of the European Convention on Human Rights, given the higher protection afforded by Article 10 to speech on matters of public interest. As we explain in Chapter 2, if an exercise of freedom of expression bears on a matter of public interest, the ECtHR will be less ready to find that an interference – especially a serious interference like a criminal conviction – will be compatible with Article 10.[439]

**Example 5: contribution to a matter of public interest**

Azi is a humanitarian campaigner and artist. He runs a popular website called "Peace Now" where he posts art pieces advocating against war. Azi's art includes images depicting war zone casualties and testimonies from those affected by conflict.

On the home page of his website, Azi explains "My art may shock, disturb, or upset you. It should. We should all be tormented by the state of the world. Let this torment be a spur to action."

5.183 In this example, it is likely that all but one of the elements of the proposed new offence are met. Azi's communications are likely to cause serious emotional distress to those likely to see, hear, or otherwise encounter them. Azi, by his own admission, intends to provoke a response that arguably amounts to at least serious emotional distress. However, given that his communications are – or, at least, are meant as – a contribution to a matter of public interest (namely, the legitimacy of war) the court should find that he has a reasonable excuse.

5.184 We are conscious that, especially in online spaces such as Twitter, polarised and highly charged exchanges take place on issues that attract a high level of public engagement. The requirement that the court must have regard to whether the

[439] See our discussion of *Perinçek v. Switzerland* (2016) 63 EHRR 6 (App No 27510/08) in Chapter 2.

communication was or was meant as a contribution to a matter of public interest will be pertinent in such contexts.

5.185 One example is exchanges between self-described “gender critical” groups and trans rights activists. In June 2020, Tweets written by J K Rowling garnered significant media attention. J K Rowling initially Tweeted in response to an opinion piece regarding additional difficulties faced by people dealing with their menstruation during the COVID-19 pandemic. She wrote: “‘People who menstruate’. I’m sure there used to be a word for those people. Someone help me out. Wumben? Wimpund? Woomud?” This statement was criticised on the basis that it reflects a transphobic attitude, implying that transgender men and non-binary people who can menstruate are women, and excluding transgender women who cannot menstruate. J K Rowling responded to these criticisms with further Tweets:

> If sex isn’t real, there’s no same-sex attraction. If sex isn’t real, the lived reality of women globally is erased. I know and love trans people, but erasing the concept of sex removes the ability of many to meaningfully discuss their lives. It isn’t hate to speak the truth.
>
> The idea that women like me, who’ve been empathetic to trans people for decades, feeling kinship because they’re vulnerable in the same way as women — ie, to male violence – ‘hate’ trans people because they think sex is real and has lived consequences — is a nonsense.
>
> I respect every trans person’s right to live any way that feels authentic and comfortable to them. I’d march with you if you were discriminated against on the basis of being trans. At the same time, my life has been shaped by being female. I do not believe it’s hateful to say so.

5.186 We do not doubt that these Tweets had the capacity to cause distress, especially to transgender people. For example, the LGBT+ organisation GLAAD responded to J K Rowling saying: “We stand with trans youth, especially those Harry Potter fans hurt by her inaccurate and cruel tweets.”

5.187 However, it seems to us that the Tweets were, or at least were meant as, a contribution to a matter of public interest. In light of this, and of the level of protection afforded to such expression under Article 10 ECHR, a court would very likely find that they were sent or posted with reasonable excuse.

5.188 As we have explained above, at 1.11, not all harmful speech warrants State sanction and there is a particularly weighty burden of justification for imposing a *criminal* sanction. That these Tweets would not be caught by our proposed offence reflects our provisional view that they do not warrant criminalisation.

**Consultation Question 12.**

5.189 We provisionally propose that the offence should specify that, when considering whether the communication was sent or posted without reasonable excuse, the court must have regard to whether the communication was or was meant as a contribution to a matter of public interest. Do consultees agree?

**Consultation Question 13.**

5.190 We invite consultees' views as to whether the new offence would be compatible with Article 10 of the European Convention on Human Rights.

## PRIVATE COMMUNICATIONS

5.191 In Chapter 2, we considered the requirements of the right to respect for private life, protected by Article 8 ECHR, as they apply to the criminalisation of communications. We said that, although some seemingly "private" communications will not fall within the scope of Article 8, many will. Any restriction on private communications within the scope of Article 8 must be in accordance with Article 8(2).

5.192 Our proposed offence does not make a distinction between public and private messages. However, the private nature of the communication will affect the practical application of the offence. A private joke between friends, even a joke in very bad taste, will not be covered unless it was likely to cause harm to someone likely to see, hear, or otherwise encounter it. In our view, the proposed offence should, therefore, be compatible with Article 8 ECHR: the interference with the rights protected under Article 8(1) would be a proportionate pursuit of a legitimate aim, such as public safety or the protection of health or morals.

5.193 In short, under the proposed new offence, private communications may be criminal if they are likely to cause harm (amounting to at least serious emotional distress), but will not be criminal if they are not likely to cause harm. Consider the following example:

**Example 6: private messages**

Two close friends, Ben and Daria, are having a private conversation over WhatsApp messenger. They start discussing the COVID-19 virus. One message from Ben to Daria says: "When you eat bats and bamboo and rats and shit and call it a 'Chinese delicacy', why'd you act surprised when diseases like coronavirus appear?" Daria replies "lol" and then sends a meme. The meme depicts two people of Chinese origin: a man with his tongue out, and a woman he is ogling. The man is labelled "coronavirus" and the woman is labelled "dirty Asian". After this, Ben and Daria's chat ends amicably.

5.194 It is very unlikely that Ben would be guilty of the proposed new offence. This is because it seems clear that neither of the mental elements of the offence are met: Ben did not intend and was not aware of a risk of harm to Daria (and, indeed, it seems unlikely that there was any such risk).

5.195 Under the first of the two alternative mental elements, Ben must have intended to cause harm to someone likely to see, hear, or otherwise encounter the communication. In this case, it seems that the only person likely to see the communication was Daria; Ben's close friend. Given the content of the message and his relationship with Daria, it seems clear that Ben intended his message as a joke between friends. It is highly unlikely that the prosecution could prove beyond reasonable doubt that Ben intended to cause harm to Daria.

5.196 Under second of the two mental elements, Ben must have been aware of a risk of harm to Daria. In this case, Ben and Daria are close friends and, as is apparent from their messages, they share a similar sense of humour. Therefore, Ben would not have been aware of a risk that Daria would be harmed by the messages – as we have said, there may not have been any such risk.

5.197 This is sufficient to show that Ben would not be guilty of the proposed new offence. If the mental element is not met, the offence is not complete, regardless of whether the conduct element – whether the communication was likely to cause harm – was met. Nor does the question of whether the communication was sent or posted with reasonable excuse arise.

5.198 The same holds true for Daria: for the same kinds of reasons, she will not be guilty of the proposed new offence.

**Example 7: secondary distribution**

The next morning, Daria takes a screenshot of her chat with Ben and sends it to her workplace WhatsApp group, which includes over 50 participants. She thinks some of her colleagues will find it funny and includes the caption "Lol! Get those dirty Asians out of our office, am I right?!".

5.199 On the facts, it is unlikely that the prosecution could prove that Daria intended to cause harm: she thought that her colleagues would find the messages funny, and her caption ("Lol!") attests to this.

5.200 However, Daria may nonetheless be guilty of the proposed new offence. This is because Daria may have been aware of a risk of harm. Daria sent the screenshot to 50 of her work colleagues. Given the size of the group and the fact that the participants were her colleagues, rather than her friends, it's unlikely that Daria knew *all* of the recipients well enough to believe that they would find the content humorous (even though she thought that at least *some* of them would find the messages funny). Therefore, she may have been aware of a risk that some of them would be caused harm (amounting to at least serious emotional distress) as a result of receiving this kind of message.

5.201 Regarding the conduct element, it's arguable that one of Daria's colleagues was likely be caused at least serious emotional distress. This would be especially likely if any of Daria's colleagues were of Chinese or Asian heritage.

5.202 The court would then have to consider whether Daria had a reasonable excuse for sending the message. The content of the message may, to the extent it can be understood as a discussion of the COVID-19 outbreak, fall under the protection for contributions to matters of public interest. This would have to be taken into account as part of the reasonableness assessment. However, the proposed new offence requires only that this factor is considered by the court: it is not determinative. Given the tenor of the conversation and the lack of social utility in sending the message, the court may well find that Daria did not have a reasonable excuse. She may, therefore, be guilty of the proposed offence.

5.203 These additional facts also cause us to ask again the question whether Ben would be guilty of the proposed new offence. Specifically, they raise the question of whether Ben was aware that Daria might share their conversation and was therefore aware of a risk of harm. If, for example, there was precedent for her doing so, it may be arguable that Ben was aware of a risk of harm to a likely audience; the likely audience being Daria's colleagues. On these facts, it seems unlikely that that Ben committed the proposed offence. However, in other cases, it may be that the "originator" or original author of the content is criminally liable, as well as the person who re-shares the content.

**Example 8: secondary distribution and "whistle-blowers"**

Robin, a colleague of Daria's, is angered by the message. She feels that it is inappropriate for a workplace WhatsApp group and is concerned about how it will affect the cohesiveness of the team. She sets out her concerns in an email to several members of senior management, with the screenshot included as an attachment.

5.204 Though the other elements of the offence may arguably have been met, Robin, unlike Daria, is likely to have a reasonable excuse for sharing the screenshot. She sent the

screenshot to her managers for the legitimate purpose of "whistle-blowing": she called potential wrongdoing to the attention of the appropriate people, in order that they might take action.

**Consultation Question 14.**

5.205 We invite consultees' views as to whether the new offence would be compatible with Article 8 of the European Convention on Human Rights.

## THREATS

5.206 The existing communications offences explicitly cover threats. Section 127(1) of the CA 2003 currently prohibits communications that are "menacing". Section 1(1)(a)(ii) of the MCA 1988 makes it an offence to send a "threatening" communication with the purpose of causing the recipient distress or anxiety. Our proposed new communications offence does not contain any explicit reference to "menacing" or "threatening" communications.

5.207 Communications that can be described as "threatening" or "menacing" seem more obviously worthy of criminalisation than "indecent" or "grossly offensive" communications. For example, Matthew Wain was recently convicted for posting a YouTube video in which he said that he hoped the National Health Service ("NHS") staff at Birmingham City Hospital would "all die of the coronavirus because they would deserve it." He also said, "Not being funny... after what I had done to me yesterday I would bomb the place, to be honest." As District Judge Briony Clarke observed, part of the wrongful nature of Mr Wain's conduct was that it was threatening.[440]

5.208 Despite its lack of explicit reference to "menacing" or "threatening" communications, our proposed new communications offence would likely cover Mr Wain's conduct. Especially given the context of COVID-19 pandemic, and the crucial role of NHS staff in responding to the crisis, a court may find that the communication was likely to cause harm to someone likely to see, hear, or otherwise encounter it: such people including not only the staff Birmingham City Hospital themselves, but perhaps also their family members, NHS staff more broadly, or even members of the wider public.

5.209 In addition, there are other offences covering threats. A threat to kill is an offence under section 16 of the Offences Against the Person Act 1861, and other threats may constitute a form of assault. For example, as we mentioned in Chapter 4, the courts have held that an assault may be committed by a defendant making a telephone call which causes a victim to fear immediate and unlawful violence.[441] Bomb hoaxes are covered by section 51 of the Criminal Law Act 1977.

5.210 In our view, then, "threatening" and "menacing" communications are sufficiently covered by a combination of our proposed new communications offence and the

---

440 See BBC News, *YouTuber jailed for Birmingham hospital bomb threat* (18 June 2020), https://www.bbc.co.uk/news/uk-england-birmingham-53092117 (last visited 09 September 2020).

441 *R v Ireland*, [1998] AC 147.

existing law. That being said, we do recognise that, in cases where a threat is covered only by our proposed new communications offence, there may be a labelling problem. Our proposed offence is framed in terms of emotional and psychological harm. It may not, therefore, adequately capture and describe the nature of the wrongdoing when it comes to threats to, for example, destroy a building or cause financial ruin. We would welcome consultees' views on whether the labelling issue is a sufficient justification for a specific offence relating to threats.

**Consultation Question 15.**

5.211 In addition to our proposed new communications offence, should there be a specific offence covering threatening communications?

## JURISDICTION

5.212 The proposed new communications offence has been drawn in such a way that the offence is complete when the defendant "sends or posts" the communication. The commission of the offence does not require that the communication is received, or that it actually causes harm amounting to at least serious emotional distress.

5.213 If, therefore, the act of sending takes place in England and Wales, the offence would be committed regardless of whether the communication is received outside the jurisdiction. This should, we think, avoid potential complications arising from the technology used to send the communication. It shouldn't matter if, for example, a sender based in London uploads a message from their laptop to a website hosted in another jurisdiction: the act of sending took place in England and Wales, so the offence took place within jurisdiction.

5.214 On the other hand, where the communication is received in England or Wales, but sent from outside of the jurisdiction, no offence is committed in England and Wales. This may, in one sense, seem undesirable. Even if harm is caused, or likely to be caused, in England and Wales, no offence is committed in England and Wales if the sender is outside of the jurisdiction. However, inclusion of a territorial provision penalising acts committed abroad seems to us to be disproportionate, given that the offence is relatively low-level. Further, although the offence is designed better to address online abuse and its harmful impacts, this is not a result offence but a conduct offence, penalising wrongful conduct committed within the jurisdiction.

**Consultation Question 16.**

5.215 Do consultees agree that the offence should not be of extra-territorial application?

# Chapter 6: Specific forms of online abuse and complementary law reforms

## INTRODUCTION

6.1 We begin this chapter by setting out proposals for reform of section 127(2) of the Communications Act 2003 ("CA 2003"). The proposed offence set out in Chapter 5 is intended to replace section 1 of the Malicious Communications Act 1988 ("MCA 1988") and section 127(1) of the Communications Act 2003 ("CA 2003"), but not section 127(2) CA 2003. It is targeted at communications likely to cause harm. We think there is scope for a further offence targeted at knowingly false communications.

6.2 Further, as we have said throughout this Consultation Paper, we have been asked to consider a number of specific behaviours. In this chapter, we consider whether these behaviours warrant a criminal law response beyond the proposed harm-based offence outlined in Chapter 5. To reiterate, the behaviours are:

(1) pile-on harassment;

(2) cyber-flashing;

(3) glorification of self-harm; and

(4) glorification of violent crime.

6.3 All of these behaviours would, at least some of the time, be caught by our proposed harm-based offence. In this chapter, we explain the reasons for this. We also explain the circumstances under which these behaviours may be caught by other, existing offences.

6.4 Nonetheless, we think there is a case for complementary law reforms to address some of these behaviours specifically. One key purpose of this chapter is to explain where, in our view, complementary reforms may be justified, and to set out proposals for such reforms.

### The proposed harm-based offence

6.5 In this chapter, we explain how the proposed harm-based offence, set out in Chapter 5, applies to some specific behaviours, and how it relates to our proposals for reform of section 127(2) CA 2003. For convenience, we restate the main elements of the offence here:

(1) the defendant sent a communication that was likely to cause harm to a likely audience;

(2) in sending the communication, the defendant intended to harm, or was aware of a risk of harming, a likely audience; and

(3) the defendant sent the communication without reasonable excuse.

(4) For the purposes of this offence, definitions are as follows:

(a) a **communication** is an electronic communication, letter, or article;

(b) a **likely audience** is someone who, at the point at which the communication was sent by the defendant, was likely to see, hear, or otherwise encounter it; and

(c) **harm** is emotional or psychological harm, amounting to at least serious emotional distress.

(5) When deciding whether the communication was likely to cause harm to a likely audience, the court must have regard to the context in which the communication was sent, including the characteristics of a likely audience.

(6) When deciding whether the defendant had a reasonable excuse for sending the communication, the court must have regard to whether the communication was a contribution to a debate in the public interest.

## SECTION 127(2) OF THE COMMUNICATIONS ACT 2003

6.6 In this section, we set out our proposals for reform of section 127(2) CA 2003. Our main proposal is for a new offence which, together with the offence in Chapter 5, forms a coherent set of offences that criminalise two types of communication: communications that are likely to cause harm, and communications that the sender knows to be false.

6.7 It is important to note that, in the case of false communications, there are already criminal offences that address more serious forms of this behaviour. For example, false representations can constitute fraud under the section 2 of the Fraud Act 2006. However, in our view there is nonetheless a role for an additional offence, without which there may be an undesirable gap in the criminal law.

### The offences under section 127(2)

6.8 Section 127(2) CA 2003 provides:

> 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.

### Proposed reform of section 127(2)

6.9 In our view, subsections 127(2)(a) and (b) CA 2003, covering false communications, and subsection 127(2)(c), covering persistent communications, warrant separate treatment. In summary, we propose that section 127(2) should be repealed and replaced with:

(1) an offence addressing knowingly false communications – currently covered by subsections 127(2)(a) and (b) – to complement the proposed harm-based offence set out in Chapter 5; and

(2) a specific offence addressing hoax calls to the emergency services, currently covered by subsection 127(2)(c).

6.10 In what follows, we explain these proposals in more detail. We will first consider the offence in section 127(2)(c), before considering the scope for reform of section 127(2)(a) and (b).

### Persistent use

6.11 As we noted in Chapter 3, one of the origins of the offence in section 127 CA 2003 lies in protection of the public communications network, to ensure that it was not abused and used to abuse members of the public. It is noteworthy that section 127(2)(c) is still used to protect public facilities in this sense: of a random sample of 26 prosecutions of 127(2)(c) sent to us by the Crown Prosecution Service ("CPS"), seventeen of them were prosecutions for repeated hoax or vexatious or trivial calls to the emergency services.

6.12 "Public electronic communications network" has subsequently been interpreted more broadly, to include privately-owned telephone networks and the internet, on the basis that they are public in nature if not ownership. This makes sense when using these offences to prevent harmful communications more generally. (For example, the remaining nine cases in the CPS's random sample of 26 offences under section 127(2)(c) were concerned with domestic abuse). Indeed, we note in Chapter 3 that the requirement that a communication be sent over a public electronic communications network is *too* restrictive as a way of addressing harms in the digital space generally.

6.13 However, the result of expanding the definition of the network – absent the theoretical underpinning of protection of a public facility – is that the 127(2)(c) offence is now incredibly broad. For example, repeatedly sending text messages to a family member for the purpose of annoying them (whether or not it did annoy them) is a criminal offence. This seems unjustifiable – neither the level of fault nor the level of harm would warrant criminal sanction. Consider the following example:

**Example 1: persistent communications sent for the purpose of causing annoyance**

Francis and Abdul are close friends. They enjoy playing pranks on each other. One afternoon, Francis decides to send Abdul a series of GIFs using Facebook messenger, to try and annoy him. The next day, Francis and Abdul meet in the pub and laugh about the incident.

6.14 Francis made persistent use of a public electronic communications network (the internet), for the purpose of annoying Abdul. Francis' conduct, despite being harmless

and non-culpable, would probably be caught by the existing offence under section 127(2)(c). This is, in our view, a clear case of over-criminalisation.

6.15 In some cases, it may be appropriate to address persistent misuse through means other than the criminal law. For example, Ofcom, the regulator for communications services, is permitted under section 128 CA 2003 to issue notifications for breaches of section 127(2)(c). Under section 129, that notification is enforceable in the *civil* courts and allows for remedies including injunctive or compensatory relief.

6.16 Where the harm clearly is more serious – hoax emergency calls and domestic abuse are examples of this – then targeted laws (tailored to the wrongful behaviour) seem a more appropriate measure than a catch-all summary offence. The Domestic Abuse Bill 2020 is an excellent example of this, particularly because it gives police the power to make a domestic abuse protection order[442] (breach of which would be a criminal offence).[443] Aspects of domestic abuse are also criminalised under section 76 of the Serious Crime Act 2015 (which addresses controlling or coercive behaviour).[444] Our proposed harm-based offence to replace section 127(1) CA 2003 (as set out in Chapter 5) would, in any case, capture communications that are likely to cause emotional or psychological harm. If the communications are persistent or part of a pattern of domestic abuse, these factors would form part of the context that the court must take into account when establishing whether harm was likely.

6.17 We therefore consider that section 127(2)(c) should be repealed. We recognise that hoax emergency calls may require specific criminal sanction absent 127(2)(c), but we believe that other genuinely harmful behaviour that would be caught under this section falls within the scope of the other offences we have identified.

**Consultation Question 17.**

6.18 We provisionally propose that section 127(2)(c) should be repealed and replaced with a specific offence to address hoax calls to the emergency services. Do consultees agree?

### Knowingly false communications

6.19 Section 127(2) CA 2003 also covers some types of false communication. Subsection 127(2) covers communications that the defendant:

(1) sends over a public electronic communications network;

(2) for the purpose of causing annoyance, inconvenience or needless anxiety to another;

442 Domestic Abuse Bill 2020, s 18.

443 Domestic Abuse Bill 2020, s 35(1).

444 See discussion in Chapter 5.

(3) and that he knows to be false.

6.20 Consider the following example:

> **Example 2: false communications sent for the purpose of causing annoyance, inconvenience or needless anxiety**
>
> Hayley has fallen out with her friend, Becky, a restaurant owner. Out of anger with Becky, and hoping to teach her a lesson, Hayley leaves several negative reviews of Becky's restaurant on Trip Advisor, using different aliases. The reviews make various false claims: that the restaurant recently had a rat infestation; that the chefs are not qualified; and that one of the waiters has a criminal record.

6.21 This kind of behaviour may be caught by section 127(2). These are messages sent by means of a public electronic communications network (the internet); that Hayley knows to be false; and that the prosecution could probably establish were sent for the purpose of causing annoyance, inconvenience, or needless anxiety to Becky.

6.22 However, we have not seen evidence to suggest that this subsection is often prosecuted.

6.23 It is also worth recalling that many offences involving false information will be prosecuted as fraud, for example, under section 2 of the Fraud Act 2006, This section may apply so long as the person making the false representation intended: (i) to make a gain for himself or another, or (ii) to cause another loss or expose them to a risk of loss. On the evidence provided in the above example, it would not be difficult to establish that Hayley intended at least to expose Becky to a risk of loss.

6.24 Nonetheless, our provisional view is that there is scope for an offence of knowingly communicating false information where the intention relates not to financial gain or loss but instead to non-financial harm (such as emotional distress). This is not to say that the existing level of intended harm is appropriate: "annoyance" and "inconvenience" in particular seem to be insufficiently harmful to meet the threshold of criminality.

6.25 At the same time, as we discuss below, we are not persuaded that the intended harm should be as high as that required for the offence we propose in Chapter 5 (intention to cause or awareness of a risk of causing at least serious emotional distress).

### False communications: the proposed new offence

6.26 In our provisional view, subsections 127(2)(a) and (b) should be replaced with a new offence addressing false communications. The elements of this new offence can be summarised as follows:

(1) the defendant sent a communication that he or she knew to be false;

(2) in sending the communication, the defendant intended to cause non-trivial emotional, psychological, or physical harm to a likely audience; and

(3) the defendant sent the communication without reasonable excuse.

(4) For the purposes of this offence, definitions are as follows:

(a) a **communication** is an electronic communication, letter, or article; and

(b) a **likely audience** is someone who, at the point at which the communication was sent by the defendant, was likely to see, hear, or otherwise encounter it.

6.27 This offence is intended to complement the proposed harm-based offence set out in Chapter 5. The two offences are similar in structure and have similar elements.

6.28 One of the main differences is that the offence to replace subsections 127(2)(a) and (b) does not require that the communication was likely to cause to harm, but instead covers only communications that the defendant knows to be false. This requirement helps to ensure that the offence catches only communications which lack social utility: knowingly false communications, short of satire and fiction, generally have little to recommend them. It also reflects a degree of culpability on the part of the defendant.

6.29 The harm component of the mental element has a correspondingly lower threshold: the defendant must intend to cause harm, where harm is any non-trivial emotional, psychological, or physical harm. This can be contrasted in with the proposed offence set out in Chapter 5, under which the defendant must intend to cause, or be aware of a risk of causing, emotional or psychological harm amounting to at least serious emotional distress.

6.30 The other main difference is that the mental element (in addition to knowledge of falsity) is intention to cause harm; awareness of a risk of harm is not sufficient for the offence to be made out. This is, we think, congruent with the other elements of the offence. In what follows, we explain the elements of the offence in more detail.

6.31 Given that this proposed offence requires neither actual nor likely harm, and the threshold of intended harm is low, our view is that it should – like the existing offences under section 127(2) – be summary only.

**Consultation Question 18.**

6.32 We provisionally propose that section 127(2)(a) and (b) of the Communications Act 2003 should be repealed and replaced with a new false communications offence with the following elements:

(1) the defendant sent a communication that he or she knew to be false;

(2) in sending the communication, the defendant intended to cause non-trivial emotional, psychological, or physical harm to a likely audience; and

(3) the defendant sent the communication without reasonable excuse.

(4) For the purposes of this offence, definitions are as follows:

(a) a **communication** is a letter, electronic communication, or article (of any description); and

(b) a **likely audience** is someone who, at the point at which the communication was sent by the defendant, was likely to see, hear, or otherwise encounter it.

Do consultees agree?

## The conduct element

6.33 In our proposal, the conduct element of the offence is that the defendant sent a communication that he or she knew to be false, where a communication is a letter, electronic communication, or article (of any description).

6.34 Of course, the requirement that the defendant knew the communication to be false comprises a mental element: knowledge of falsity. However, it also comprises a conduct element: if the defendant *knows* rather than *believes* the communication to be false, then the communication must actually *be* false. In any case, the requirement that the communication must be false is made explicit in the drafting of our proposal, as it is in the drafting of section 127(2)(a): the phrasing is, "knows *to be* false".

6.35 For the purposes of a new offence covering false communications, we do not think that the "public electronic communications network" requirement in subsection 127(2)(a) should be replicated.

6.36 As we explain in Chapter 3 (and revisit above) the "public electronic communications network" requirement under section 127(1) makes an arbitrary distinction between potentially equally harmful modes of communication. A similar problem also arises in the case of section 127(2): false (or, indeed, persistent) messages sent for malign purposes are not necessarily any less problematic for being sent by, say, Bluetooth or a work intranet rather than the internet.

6.37 Instead, the proposed new offence applies to any communication sent by the defendant (provided the defendant knows the communication to be false, and the additional aspects of the mental element – explained below – are met). In this sense, it is the same in scope as the proposed harm-based offence set out in Chapter 5.

**Consultation Question 19.**

6.38 We provisionally propose that the conduct element of the false communications offence should be that the defendant sent a false communication, where a communication is a letter, electronic communication, or article (of any description). Do consultees agree?

### The mental element:

6.39 In our proposal, the mental element of the offence is:

(1) the defendant knew the communication to be false; and

(2) the defendant, in sending the message, intended to harm a likely audience, where harm is defined as any non-trivial emotional, psychological, or physical harm.

6.40 In what follows, we discuss the reasoning behind each aspect of the mental element.

#### Knowledge of falsity

6.41 Subsections 127(2)(a) and (b) do not cover communications that the sender believes to be true. For example, the conduct of someone who sincerely believes that vaccinating a child against various illnesses is bad for the child's health, and sends messages to this effect, would not be caught.

6.42 In our provisional view, any replacement offence should replicate the requirement that the defendant knew the communication to be false. The main reason for this is to ensure that the offence reflects a sufficient degree of culpability on the part of the defendant. As we have emphasised throughout this Consultation Paper, an element of culpability is essential to justify criminalisation. The Criminal Offences Gateway Guidance stipulates that the criminalised behaviour must be sufficiently serious to merit the stigma associated with a criminal conviction.[445]

6.43 In modern terminology, knowingly false communications are sometimes described as "disinformation", as distinct from "misinformation". While disinformation is *deliberately* misleading, misinformation is not.[446] Misinformation is being tackled by other

---

445 Ministry of Justice, Criminal Offences Gateway Guidance (08.11). Available at https://www.justice.gov.uk/downloads/legislation/criminal-offences-gateway-guidance.pdf (last visited 09 September 2020).

446 Cambridge Dictionary defines "disinformation" as false information spread in order to deceive people. Available at https://dictionary.cambridge.org/dictionary/english/disinformation (last visited 09 September 2020).

mechanisms, aside from the criminal law. For example, in 2017, the organisation First Draft produced a *"Fake News" Field Guide*, to enhance public understanding of the scope, nature and composition of misinformation.[447] More recently, First Draft produced *Too much information: A guide to navigating the infodemic*, to "help everyone have better informed conversations with family and friends about the [COVID-19] pandemic".[448] In addition, the Centre for Countering Digital Hate, in conjunction with Restless Development, has started the Youth Against Misinformation initiative. Such initiatives seem to us to be more appropriate mechanisms for dealing with false communications that the sender sincerely believes to be true.

6.44 If, however, the defendant knows that the message is false (and the sends the message for a malign purpose or with malign intent) there may be a role for the criminal law. As we have explained, section 127(2) CA 2003 already covers some communications of this kind. In our view, a replacement offence should likewise cover a subset of so-called disinformation – that is, knowingly false communications, sent with malign intent – but not misinformation.

### Raising the threshold of (intended) harm

6.45 Our proposal aims to raise the threshold of intended harm. Under the existing offence, it is a crime to send a knowingly false communication for the purpose of causing "annoyance, inconvenience or needless anxiety" to another. This is a low threshold. In our provisional view, it is too low. We therefore propose to raise the threshold to "non-trivial emotional, psychological, or physical harm".

6.46 Admittedly, the offence already requires that the defendant knows the communication to be false. In light of the potential culpability reflected in this requirement it is, in our view, appropriate that the threshold of intended harm should be on the lower end of the scale. However, we do not think that the threshold should be as low as "annoyance, inconvenience, or needless anxiety". We mean for "non-trivial emotional, psychological, or physical harm" to include, for example, distress and anxiety, but not annoyance or inconvenience which in our provisional view do not justify the imposition of a criminal sanction.

### Expanding the range of (intended) harms

6.47 Although our proposals raise the threshold of intended harm, they also expand the range of intended harms.

6.48 Aside from the "public electronic communications network" requirement, the main limitation of the existing section 127(2) offence is that it covers only a narrow range of harmful purposes. At present, the offence only covers false information sent for the purpose of causing annoyance, inconvenience, or needless anxiety. There is an argument that this makes the offence too restrictive: a defendant might send false information for another, equally if not more harmful, purpose, but this would not be caught by the offence. Consider the following example:

---

447 See https://firstdraftnews.org/project/field-guide-fake-news/ (last visited 9 September 2020).

448 See https://firstdraftnews.org/project/too-much-information-a-public-guide/ (last visited 9 September 2020).

**Example 3: false communications causing physical harm**

Mitchell posts a message on his Facebook page, telling people that injecting antiseptic will cure coronavirus. He knows that this is not true. He also knows that injecting antiseptic is very dangerous.

6.49 In this example, Mitchell's conduct will not be caught by section 127(2), unless the prosecution can show that Mitchell sent the communication for the purpose of causing annoyance, inconvenience, or needless anxiety. This will be difficult to prove. Mitchell knew that the messages were false and dangerous, but there's nothing to suggest that his purpose was to cause annoyance, inconvenience, or needless anxiety. The prosecution could plausibly argue that his purpose was to cause physical harm. However, even if this could be proved, this would still not meet the requirements of the offence. It may seem odd, and unfair, that the conduct of a defendant with a less malign purpose – like causing inconvenience – is caught by section 127(2), but Mitchell's conduct is not.

6.50 In some cases, conduct like Mitchell's may be covered by other existing offences. We mentioned in Chapter 4 that the current law regarding offences against the person covers, at least in principle, three kinds of communication: [449]

(1) communications directly causing a recognised psychiatric illness;

(2) communications which are otherwise assaults; and

(3) communications causing a person to take a poison or other destructive or noxious thing.

6.51 In Mitchell's case, the most relevant category is the third. Unlawfully and maliciously administering or *causing the taking* by any other person of any poison, or other destructive or noxious thing, so as thereby to endanger their life or to inflict any grievous bodily harm, is an offence under section 23 of the Offences Against the Person Act 1861 ("OAPA 1861"), carrying a maximum sentence of 10 years' imprisonment.

6.52 Doing the same act, unlawfully and maliciously, and with the intent to injure, aggrieve or annoy such a person, (and whether or not any harm is caused) is an offence under section 24 of the OAPA 1861, carrying a maximum sentence of 5 years' imprisonment.

6.53 The issue of causation is a potential barrier to applying these offences in situation like Mitchell's, where a defendant communicates with another person, potentially leading the other person to take a noxious thing. This issue was considered in *R v Kennedy*

[449] See the discussion in Chapter 4, from para 125.

*(No.2)*.[450] In *R v Kennedy (No.2),* the House of Lords said that, generally, the criminal law "assumes the existence of free will".[451] Where a defendant facilitates or encourages another person to take a noxious thing, the defendant may not be guilty of an offence because the law treats the other person's act as being of their own free will. This breaks the chain of causation. In such a case, the defendant would not commit an offence because it was not the defendant's act, but the other person's decision, that caused them to take the noxious thing.

6.54 Hence, in *R v Kennedy (No.2)*, in which the defendant had supplied, prepared, and passed a syringe of heroin to another person, who then injected themselves with the syringe, the defendant had not committed an offence under section 23 of the OAPA 1861, because they had neither administered nor caused the taking of the noxious thing.

6.55 There are exceptions to this. Exceptions apply to the young and to those who for any reason are not fully responsible for their actions. They also apply to the vulnerable: to those who are in situations of duress, necessity, deception, or mistake. Generally speaking, only informed adults of sound mind are treated by the criminal law as autonomous beings able to make their own decisions.[452]

6.56 Such exceptions might apply in a case like Mitchell's. If a defendant tells a victim that a noxious substance has health-giving properties, knowing that this is false, then the victim might not be treated as being informed. An uninformed act might not break the chain of causation. The defendant's communication would therefore be treated as having caused the taking of the noxious thing and the defendant could be guilty of an offence under section 23 or section 24 of the OAPA 1861.

6.57 Even so, it seems to us appropriate that there should be a low-level communications offence available to tackle conduct like Mitchell's, especially where no harm in fact eventuated. An individual message amounting to disinformation may not often result in actual emotional, physical, or psychological harm, but the wider phenomenon is a social ill that the criminal law could have some role in helping to address.

6.58 Disinformation is a widespread problem, especially in the online environment, and increasingly so.[453] For example, Chatham House writes:

> The recent re-emergence of interest in disinformation is not because the idea is novel – rather, there is a growing consensus that the digital revolution has greatly enhanced public vulnerability to manipulation by information, and action needs to be taken to counter it.[454]

6.59 The existing offence under section 127(2), despite covering some false communications, is largely impotent in addressing this problem, due to the limited

---

450 [2007] UKHL 38, [2008] 1 AC 269.

451 Above, at [14].

452 Above, at [14].

453 See, for example, https://www.theguardian.com/world/2020/apr/24/coronavirus-sparks-perfect-storm-of-state-led-disinformation (last visited 9 September 2020).

454 See https://www.chathamhouse.org/research/topics/disinformation# (last visited 9 September 2020).

range of harmful purposes it encompasses. In our proposal, therefore, "harm", as a component of the mental element, is any non-trivial emotional, psychological, or physical harm. This, we think, will equip the criminal justice system with a tool to address more effectively harmful and malign disinformation.

6.60 We do not, however, propose to cover communications that the defendant believes to be true – no matter how dangerous those communications may be. We recognise that misinformation and 'fake news' are serious social problems, but they lie beyond our Terms of Reference.

6.61 In summary, there are two main problems with the mental element under the section 127(2) offence: the threshold of harm is too low; but the range of harms is too narrow. Our proposals aim to rectify both of these problems.

### Intention rather than purpose

6.62 A further departure from section 127(2) is the reframing of the mental element in terms of "intention", rather than "purpose". As we explain in Chapter 5, we have misgivings about the use of "purpose", on the grounds that it may allow the defendant unfairly to escape liability, by citing some other, ulterior motive.

6.63 Another option would be for our proposals in relation to false communications to mirror our proposals in Chapter 5 by having a dual mental element, with "awareness of a risk of harm" as an alternative to "intention". However, unlike in the proposed harm-based offence set out in Chapter 5, our proposed false communications offence does not include a requirement that the communication was likely to cause harm. In our provisional view, false communications, unlike abusive communications, may not be worthy of criminalisation if the defendant did not intend but was merely aware of risk of harm.

**Consultation Question 20.**

6.64 We provisionally propose that the mental element of the false communications offence should be:

(1) the defendant knew the communication to be false; and

(2) the defendant, in sending the message, intended to harm a likely audience, where harm is defined as any non-trivial emotional, psychological, or physical harm.

Do consultees agree?

### Reasonable excuse

6.65 As we explain above the existing offence(s) under section 127(2) are very broad. Our proposed false communications offence is less broad. We have, as we explain above, raised the threshold of harm that the defendant must have intended to cause in sending the communication.

6.66 In addition, to protect freedom of expression and to ensure compatibility with Article 10 of the European Convention on Human Rights ("ECHR"), we propose that the new offence should – like the proposed harm-based offence set out in Chapter 5 – include a requirement that the communication was sent without reasonable excuse. In our view, the protection provided by this requirement will sometimes be important, even if the defendant intended to cause harm (for discussion on this point, see Chapter 5).

**Consultation Question 21.**

6.67 We provisionally propose that the false communications offence should include a requirement that the communication was sent without reasonable excuse. Do consultees agree?

## GROUP HARASSMENT

6.68 In this section, we explain, first, the phenomenon of group harassment, especially online. Second, we explain the circumstances under which group harassment will be caught by the existing law or by our proposed harm-based offence. Finally, we consider whether there is nonetheless a case for a specific offence to address group harassment.

### Group harassment online: behaviour and harms

6.69 As we explain in the Scoping Report and in Chapter 3, group harassment can take two forms: coordinated or uncoordinated.

6.70 By coordinated group harassment, we mean a situation in which multiple individuals act in concert to send communications that are harassing in nature to a victim. Of course, harassment need not take the form of sending communications: other types of conduct can also constitute harassment (for further discussion, see Chapter 3). However, for our purposes, the relevant type of conduct is the sending of communications.

6.71 Uncoordinated or pile-on harassment occurs when multiple individuals, acting separately, send communications that are harassing in nature to a victim. For example, hundreds of individuals sent messages to Jess Phillips MP along the lines of "I would not rape you".[455] This phenomenon is relatively unique to the online environment.

6.72 As we said in the Scoping Report, and in Chapter 4, group harassment, whether coordinated or uncoordinated, can have a serious impact: arguably more so than harassment by an individual, since harassment committed by a group can have a level

[455] 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 (last visited 9 September 2020).

of “persistence and escalation” that would be difficult for a single individual to replicate.[456]

6.73 As well as direct emotional and psychological harms, pile-on harassment is particularly likely to cause wider societal harms, in the form of a chilling effect on participation in public life.

6.74 For example, Amnesty International has conducted research tracking abuse against women MPs in the lead up to the 2017 election[457] and produced their 2018 *Toxic Twitter* report.[458] More recently, Amnesty International has reported on the huge levels of online abuse against black women MPs for defending Black Lives Matter protests and the risk this poses to public and political life:

> The content of this abuse can be extremely disturbing - including death and rape threats - and have a chilling effect on people’s willingness to speak out.
>
> These vicious attempts to silence black MPs must be met with action. Racist online abuse must be called out and properly tackled, and social media companies like Twitter must do far more to combat this extremely worrying trend, so that women can feel safe to participate in public debate and politics.[459]

### Is group harassment adequately addressed?

6.75 In some cases, group harassment may be caught by the existing law. *Coordinated* group harassment is covered by section 7(3A) of the Protection from Harassment Act 1997 (“PHA 1997”) – for a full discussion, see Chapter 3.

6.76 Individual communications that form part of an *uncoordinated* pile-on are not covered by the PHA 1997. They would sometimes be covered by the current communications offences, and are also likely to be covered by our proposed harm-based offence. In many cases, we envisage that the conduct of someone who witnesses the harassment occurring and “piles on”, without being part of any concerted effort, may be caught by the proposed offence.

6.77 In what follows, we use examples to show how the existing law, and our proposed harm-based offence, apply to group harassment.

---

456 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, at para 3.78.

457 Amnesty International UK, *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/ (last visited 09 September 2020).

458 Amnesty International, *Toxic Twitter* (2018), available at https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/ (last visited 09 September 2020).

459 Amnesty International, *UK: online abuse against black women MPs 'chilling'* (09 June 2020), https://www.amnesty.org.uk/press-releases/uk-online-abuse-against-black-women-mps-chilling (last visited 9 September 2020).

**Example 4: coordinated group harassment**

A female MP, Ruby, recently made a statement calling for the close of the gender pay gap. Within 48 hours of making the statement, Ruby received thousands of emails, Tweets, and comments on her Instagram page. Some criticised her position on the gender pay gap. Others used misogynistic slurs, calling her a "stupid slut" or a "dumb bitch". Some used the hashtag "#IwouldnotevenrapeRuby". Ruby has been vocal on her own social media pages and in the press about the abuse she has received.

As it turns out, many of the Tweets were sent by people who were part of a 4chan thread created by Oscar. Oscar wrote: "We need to teach Ruby a lesson. The world should know what a dumb slut she is. Say it loud, say it clear! "#dumbbitch #IwouldnotevenrapeRuby… You know what to do." Using an alias, he then Tweeted Ruby using the hashtags #dumbbitch and #IwouldnotevenrapeRuby.

6.78 Oscar would be likely to be guilty of the existing offence of harassment under the PHA 1997. This is because Oscar may be found to have counselled or procured the conduct of those who saw his 4chan thread and subsequently sent harassing Tweets to Ruby. Therefore, even though Oscar himself sent only one Tweet to Ruby, the Tweets of others who saw his 4chan thread must, under section 7(3A) PHA 1997, be taken to be part of his course of conduct.

**Example 5: uncoordinated group harassment**

Naomi, a young woman who follows Ruby on Twitter and Instagram, sees the harassing messages being sent to her and decides to join in. Underneath one of Ruby's Instagram posts, she comments: "You stupid slut. She-devils like you need a good raping… but I wouldn't want to be the one to do it #IwouldnotevenrapeRuby".

6.79 Naomi's comment would not be caught by section 7(3A) PHA 1997. This is because she was not part of and did not see the 4chan thread; she merely observed the pile-on and joined in. Unlike Oscar, she did not counsel or procure the conduct of other participants in the pile-on. However, Naomi's comment would likely be caught by the current communications offences, and the proposed offence. Given the nature of Naomi's comment, the prosecution may be able to prove that Naomi intended to cause harm amounting to at least serious emotional distress. Alternatively, it is very likely that she was aware of a risk that Ruby would be caused harm.

6.80 Regarding the conduct element, the comment was made in the context of a pile-on, which (as we have explained) can have a serious impact. We also note that the marginal harm caused by each individual communication does not necessarily diminish after a high volume of communications has already been received. Especially given that the comment was made in the context of a pile-on, the court should find that

the comment was likely to cause harm amounting to at least serious emotional distress.

6.81 Finally, despite being made in the wake of Ruby's statement on the gender pay gap, this particular comment was not a genuine contribution to political debate (and, it seems, was not intended as such): it was purely derogatory, and contained no remarks about Ruby's political positions of any kind. It would not, therefore, be covered by the protection for political speech. It is highly unlikely that the court would find that Naomi had a reasonable excuse for posting the comment.

**Example 6: political commentary**

A political commentator, Mohammed, is not convinced by Ruby's analysis of the gender pay gap. He is aware of the abuse she has received. He writes a Tweet directed to Ruby saying, "Good effort @RubyMP, but we need smarter thinking on this important issue" with a link to an article he wrote about the causes of gendered income inequality**.**

6.82 Mohammed's Tweet would not be caught by the proposed harm-based offence. Mohammed did not have any intention to cause Ruby harm – instead, he wanted to point out the flaws in her analysis of the gender pay gap.

6.83 Mohammed may have been aware of a risk that Ruby would be caused harm (that is, emotional or psychological harm amounting to at least serious emotional distress): he sent a Tweet which was critical of Ruby and, arguably, patronising in tone in the context of a pile-on. Moreover, Ruby had been vocal about the abuse she has received and Mohammed knew about her experience.

6.84 Even so, Mohammed had a reasonable excuse. This is because all the facts suggest that his Tweet was a genuine contribution to a political debate and was intended as such. Even without the explicit protection for political speech provided under the proposed harm-based offence, a court would probably find that taking the risk of harming Ruby was not unreasonable, given the nature of the Tweet. With the explicit protection for political speech, it is clear that Mohammed's Tweet should not be caught by the proposed offence: it was sent with reasonable excuse.

### Is there justification for a specific offence to address group harassment?

6.85 We have considered two possible offences, specifically to address group harassment. These two possibilities are:

(1) an offence criminalising the incitement or encouragement of group harassment; and

(2) an offence criminalising the conduct of those who knowingly participate in a pile-on.

6.86 In our provisional view, there is a good case to be made for an offence of the first kind, but not for an offence of the second kind.

### Incitement or encouragement of group harassment

6.87 There are two forms of conduct which may not be adequately covered by either the existing law or our proposed harm-based offence. The first type of conduct involves a defendant who coordinates but does not participate in a pile-on. Consider again Example 4: the pile-on harassment of Ruby, organised by Oscar in a 4chan thread. In this example, Oscar was guilty of harassment on the basis of the definition provided under section 7(3A) PHA 1997. However, in Example 4, Oscar himself sent an abusive Tweet to Ruby. As we noted in the Scoping Report,[460] and in Chapter 3, section 7(3A) seems rarely if ever to be prosecuted, even when defendants have themselves sent a harassing message, let alone when they have not. This is likely due to the complex drafting of section 7(3A), combined with the fact that it is a relatively low-level offence. Hence, if Oscar had not sent a Tweet to Ruby, but had merely coordinated the harassment, it seems highly unlikely that he would be prosecuted under section 7(3A).

6.88 Oscar's conduct would not be caught by our proposed harm-based offence, either – at least, not in most cases. This is because communications coordinating a pile-on will tend not to be likely to cause serious emotional distress *to a likely audience*: harm is generally caused to the target of the pile-on, not to the participants. In this situation, then, the participants in the pile-on could be prosecuted, but the instigator may escape criminal liability. This seems unfair.

6.89 That being said, there are existing criminal law mechanisms for dealing with this problem. Section 8 of the Accessories and Abettors Act 1861 ("AAA 1861") applies to any indictable offence – it would therefore include our proposed harm-based offence – and provides that anyone who aids, abets, counsels, or procures an offence is criminally liable as if they themselves had completed the criminal act. Hence, if someone who sees Oscar's 4chan thread then goes on to commit our proposed harm-based offence, Oscar could, under section 8 AAA 1861, be liable as a principal offender (that is, he would be liable as if he were the person who sent the criminal communication).

6.90 The second, and related, type of conduct is unsuccessful encouragement of a pile-on. In this variant of Example 4, Oscar sets up the 4chan thread, but nobody acts on his encouragement. Here, Oscar would not be liable under section 7(3A) PHA 1997, and nor would he be liable under our proposed offence (unless the prosecution managed successfully to argue that someone likely to see Oscar's 4chan message was likely to be caused harm).

6.91 In these variants of Example 4, Oscar may be guilty of an inchoate offence. As we note in the Scoping Report, CPS prosecution guidelines suggest that "Those who encourage communications offences, for instance by way of a coordinated attack on a person, may be liable to prosecution under the provisions of sections 44 to 46 Serious Crime Act 2007."[461] The same would hold true for our proposed offence: someone

---

460 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, paras 8.46-8.47.

461 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 (last visited 9 September 2020).

who encourages the commission of the proposed offence may be liable under the Serious Crime Act 2007 ("SCA 2007").

6.92 Under section 44 SCA 2007 it is an offence to do an act capable of encouraging or assisting an offence intending that it should be committed. Section 44 provides:

> (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.

6.93 Section 45 SCA 2007 concerns encouraging or assisting an offence believing it will be committed. Section 45 provides:

> (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.

6.94 Section 46 SCA 2007 concerns encouraging or assisting multiple offences, believing that one or more will be committed. Section 46 provides:

> (1) A person commits an offence if–
>
> > (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.

6.95 In theory, then, Oscar could be charged under one of sections 45 to 46 SCA 2007, with encouraging our proposed harm-based offence.

6.96 However, we are not aware of any prosecutions for encouraging – or aiding, abetting, counselling or procuring – the existing communications offences (regardless of

whether the encouragement, or procurement, was successful in bringing about a communications offence). The complexity of such charges may be seen as disproportionate to the gravity of the encouraged offence. The proposed offence, like section 1 of the Malicious Communications Act 1988, would be an "either-way"[462] offence. Therefore, the same point about proportionality applies: the CPS may regard it as disproportionate to prosecute inchoate forms of the proposed offence.

6.97 Moreover, although some individual messages constituting part of a pile-on may – by virtue of the requirement that context must be taken into account when assessing whether the communication was likely to cause harm – be caught by our proposed offence, this offence does not *specifically* criminalise pile-on harassment. It might, therefore, be difficult to prove that Oscar intended or believed a criminal offence would be committed.

6.98 These considerations – in conjunction with what we have heard about the prevalence and harmful impact of pile-on harassment, combined with seemingly few prosecutions for such conduct[463] – have led us provisionally to conclude that may be a case for a specific offence of incitement or encouragement of pile-on harassment.

**Consultation Question 22.**

6.99 Should there be a specific offence of inciting or encouraging group harassment?

### Knowing participation in a pile-on

6.100 As we noted in our Scoping Report, there is no specific offence dealing with the situation where a single person sends a single abusive message that does not by itself meet the criminal threshold:

(1) in the knowledge that similar abuse is being targeted at the victim; and

(2) with an awareness of the risk of greater harm to the victim occasioned by their conduct in the circumstances.[464]

6.101 There are various challenges in creating an offence criminalising each of the individual messages that constitute a pile-on. First, it is not clear how, in practice, conditions (1) and (2) – or something similar – could be evidenced. If the defendant's message were sent after one thousand similar messages had also been sent, we may be sceptical of any suggestion that the defendant was unaware that they were contributing to a course of harassment. However, this has the slightly odd effect of criminalising those

---

462 An either-way offence is one that can be tried either in the magistrates' courts or in the Crown Court. If the magistrates decide their sentencing powers are sufficient to deal with the offence, the accused may choose to have it dealt with summarily in the magistrates' court or on indictment (trial by jury) in the Crown Court.

463 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, paras 8.206-8.207.

464 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, para 8.207.

who send messages later in time while potentially allowing those who began the harassment to evade liability.

6.102 A further problem is that, in the case of an uncoordinated pile-on, unlike the section 7(3A) PHA 1997 offence, the messages are not connected by the fact that the first defendant aided, abetted, counselled or procured the conduct of the second defendant. So, we would need to think about how to define the relationship between the second defendant's message and the first defendant's message, such that they form part of the same course of conduct.

6.103 One way to do this is by similarity of content. But this presents difficulties of its own: when is a message sufficiently similar to an earlier message to form part of the same course of conduct? Recently, in the case of *Glawischnig-Piesczek v Facebook Ireland Limited*, the ECJ considered the meaning of the term "equivalent content", in the context of obligations on the part of social media platforms to remove unlawful defamatory content. The Advocate General recognized that the term "equivalent information" "gives rise to difficulties of interpretation", but found that it refers to content which "scarcely diverges from the original information" or "to situations in which the message remains essentially unaltered."[465] Hence, messages with typographical errors or slightly altered syntax or punctuation are "equivalent". This, however, seems too narrow for our purposes, as it risks excluding messages of a similar tone or theme but which use substantially different language.

6.104 These problems have led us provisionally to conclude that there is not sufficient justification for a specific offence criminalising knowing participation in a pile-on. As we have explained above, many of the individual messages constituting a pile-on will in any case be caught by our proposed harm-based offence. In our view, this proposed new offence, perhaps in combination with a specific offence of incitement or encouragement of pile-on harassment, would adequately address the problem.

**Consultation Question 23.**

6.105 Should there be a specific offence criminalising knowing participation in uncoordinated group ("pile-on") harassment?

## CYBER-FLASHING

6.106 As we mentioned in Chapter 3, reports of cyber-flashing – that is, the unsolicited sending of sexual images using digital technology – have increased in recent years. According to figures from the British Transport Police, in 2019 there were 66 reports of cyber-flashing, compared to 34 reports in 2018, and just 3 reports in 2016.[466]

---

465 Case C-18/18 [2019] ECR I-458 at [67].

466 See R Speare-Cole, *Spike in unsolicited sexual photos sent over AirDrop on trains, data reveals* (19 February 2020), available at https://www.standard.co.uk/news/crime/cyberflashing-trains-british-transport-police-a4365886.html (last visited 09 September 2020).

Especially given this increase in reported incidents of cyber-flashing, our view is that this type of online communication requires specific consideration.

6.107 In this section, we explain, first, the phenomenon of cyber-flashing and the attendant harms. Second, we explain the circumstances under which cyber-flashing will be caught by the exposure offence in section 66 of the Sexual Offences Act 2003. Third, we consider whether cyber-flashing would be caught by our proposed harm-based offence. Finally, we explain why there is nonetheless a case for further reform of the law. Specifically, we consider whether and how the exposure offence under section 66 of the Sexual Offences Act 2003 can be amended to include cyber-flashing.

### Cyber-flashing: behaviour and harms

6.108 As we explain in Chapter 4, we have learned from stakeholders that the term "cyber-flashing" is used to refer to a range of behaviours, but mostly commonly involves a man sending an unsolicited picture of his genitals to a woman. One well-documented and seemingly prevalent form of this behaviour involves the sending of such images via Apple's "AirDrop" function: this mode of communication, and others like it, allows perpetrators to access a wider range of potential recipients, with whom they have no prior relationship.[467]

6.109 In Chapter 4, we set out testimony, collected by Sophie Gallagher, from women who have been subjected to cyber-flashing.[468] This testimony makes clear the negative emotional and psychological impact that such behaviour can have, with responses such as fear, shame, and disgust sometimes lasting in the longer term, far beyond the timeframe of an individual incident.

6.110 Further, we have been told by Professor Clare McGlynn and Dr Kelly Johnson that cyber-flashing is experienced as a form of sexual harassment, involving coercive sexual intrusion by men into women's everyday lives. Indeed, this is illustrated in some of the aforementioned testimony:

> "The normality of this sexually aggressive behaviour is such that I am not massively surprised [when it happens] and over time I have built up a defence mechanism of laughing it off. But at its core it is very invasive."[469]

> "It was only later I realised how predatory that cyber flashing behaviour was."[470]

6.111 In particular, it is experienced in much the same way as offline forms of indecent exposure:

---

467 See, for example, S Gallagher, *Will Apple ios13 make it Easier for Cyberflashers to Target Victims* (24 September 2019) available at https://www.huffingtonpost.co.uk/entry/will-apple-ios-13-make-it-easier-for-cyber-flashers-to-target-victims_uk_5d8381a0e4b0849d4724c19c (lasted visited 9 September 2020).

468 S Gallagher, *70 Women On What It's Like To Be Sent Unsolicited Dick Pics*, (12 July 2019), available at https://www.huffingtonpost.co.uk/entry/cyberflashing-70-women-on-what-its-like-to-be-sent-unsolicited-dick-pics_uk_5cd59005e4b0705e47db0195 (lasted visited 9 September 2020).

469 Amy Martin, 25, London, on AirDrop on the street.

470 Mared Parry, 21, Wales, on Facebook Messenger.

> "It felt like this was another harassment women just have to absorb. It should work like any indecent exposure."[471]
>
> "It is the same as physical exposure and it should be treated as such."[472]

6.112 In short, the research suggests that cyber-flashing causes significant harms, akin to other sexual offences, particularly offline or "real time" forms of indecent exposure.

### Is cyber-flashing adequately addressed by the Sexual Offences Act?

6.113 Exposure – colloquially known as "flashing" – is criminalised under section 66 of the Sexual Offences Act 2003 ("SOA 2003"). Section 66(1) provides:

> A person commits an offence if—
>
> (a) he intentionally exposes his genitals, and
>
> (b) he intends that someone will see them and be caused alarm or distress.

6.114 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.[473]

6.115 The offence under section 66 SOA 2003 can apply to online communications. For example, in *R v Alderton,*[474] the defendant pleaded guilty to six counts of exposure under section 66 SOA 2003, for exposing his genitals to the victim via "Facetime" (the iPhone's live video calling service). The appeal concerned the sentence-length only.

6.116 In *R v Alderton*,[475] the defendant exposed his genitals via "live stream". In many cases, though, cyber-flashing involves the distribution of images or recordings of the perpetrator's genitals: the perpetrator does not expose his genitals in real time. As we note in the Scoping Report, whether the offence under section 66 SOA 2003 covers this type of conduct – where the "exposure" does not take place in real time – has yet to be tested.[476] Therefore, there is a risk that cyber-flashing – the harms of which are akin to the sexual offences – is unable to be prosecuted as such.

### Is cyber-flashing adequately addressed by our proposed harm-based offence?

6.117 Provided the defendant intended or was aware of a risk of harm, cyber-flashing will likely be caught by our proposed harm-based offence.

---

471 Kate O'Sullivan, 37, Edinburgh, on AirDrop on an aeroplane.

472 Gail Watt, 37, London, on AirDrop on the London Underground.

473 Sexual Offences Act 2003, s 66(2).

474 [2014] EWCA Crim 2204.

475 [2014] EWCA Crim 2204.

476 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, para 6.144.

**Example 7: cyber-flashing**

Jack and Sonya are strangers riding in a quiet London Overground carriage, along with several other men but no other women. Jack finds Sonya very attractive and hopes that she finds him attractive, too. Using the AirDrop function on his iPhone, Jack discovers another iPhone within range called "Sonya's phone". Assuming correctly that the phone belongs to Sonya (the only woman in the carriage), Jack uses AirDrop to send to this phone a photograph of his erect penis (which he had previously taken and saved).

A notification appears on Sonya's phone with the text "Jack would like to share a photo" and a preview of the image, clearly depicting his penis. Sonya selects the option to "decline" the photograph. She doesn't know which of the men in the carriage was the sender, but she can see Jack smiling at her. She is visibly frightened and gets off the train at the next stop. Jack is disappointed that his behaviour, which he saw as a sexual advance, caused this reaction from Sonya.

6.118 Jack did not have any intention to cause harm. Instead, he hoped – however misguidedly – that he would be making a welcome sexual advance.

6.119 However, Jack's behaviour would likely be caught by the proposed new offence. The prosecution should be able to prove that Jack's behaviour was likely to cause Sonya emotional and psychological harm amounting to at least serious emotional distress.

6.120 It is also likely that Jack was aware of a risk of harm; certainly, he had no reasonable grounds for believing that Sonya had consented to or would welcome such contact.

6.121 Finally, Jack's communication obviously does not fall within the protection for political speech, nor do there seem to be any other grounds for arguing that he has a reasonable excuse.

**Example 8: maliciously motivated cyber-flashing**

The following week, Sonya has the misfortune of being subject to another instance of cyber-flashing. This time, the perpetrator is Jimmy. Jimmy has various photographs of his genitals saved to his iPhone. Whenever he rides the Overground, he routinely uses AirDrop to send the pictures to whichever iPhones are within range. He enjoys seeing the reactions of fear or distress.

6.122 Jimmy's behaviour would likely be caught by the proposed new offence. Unlike Jack, Jimmy intends to cause harm: he acts in order to elicit fear or distress. Given his higher level of culpability, Jimmy should also face a heavier sentence than Jack.

### Benefits of making cyber-flashing a sexual offence

6.123 Whilst cyber-flashing involving the distribution of images or recordings will be caught by our proposed new offence (provided the mental element is met), there is nonetheless a case for making cyber-flashing a specific sexual offence.

6.124 There are two main reasons for this. The first reason is a matter of fair labelling. Cyber-flashing is, as a matter of common sense, conduct of a sexual nature. Further, as we note in Chapter 4 and above, those who have been subjected to cyberflashing compare its impact to that of other sexual offences: for example, it can cause similar feelings of violation and sexual intrusion. Our proposed harm-based offence does not fully reflect this specifically sexual behaviour and harm. It covers a wide range of abusive communications, some of which may be sexual, and some of which are not. In our provisional view, there should be a clear option to prosecute cyber-flashing as a sexual offence in order to ensure that the nature of the offending conduct is more accurately labelled by the offence.

6.125 The second reason concerns the additional legal protections that apply in respect of sexual offences. Under section 103A SOA 2003, inserted by the Anti-social Behaviour, Crime and Policing Act 2014, these protections include Sexual Harm Prevention Orders: orders made by the court to protect the public or members of the public from the risk of sexual harm presented by a defendant. Under Section 103A, a court may make a Sexual Harm Prevention Order in respect of offences listed in Schedules 3 and 5, if it is satisfied that this is necessary for the purpose of:

(1) protecting the public or any particular members of the public from sexual harm from the defendant, or

(2) protecting children or vulnerable adults generally, or any particular children or vulnerable adults, from sexual harm from the defendant outside the United Kingdom.

6.126 In short, if a given form of conduct is treated as a sexual offence, this has various consequences during the investigation, at trial and after conviction. In our view, it seems appropriate for such consequences – such as Sexual Harm Prevention Orders – to attend to cases of cyber-flashing.

6.127 Therefore, our provisional view is that cyber-flashing should be a sexual offence, carrying with it an appropriate range of sentencing options.

### Can this be achieved by amending section 66 SOA 2003 (exposure)?

6.128 One of the easiest ways of addressing the gap in the law would simply be to amend section 66 of the SOA 2003 to clarify that it covers digital exposure, whether live or otherwise.

6.129 We do not consider that this would represent an unjustifiable expansion of the law. The crime is one of specific intent – the perpetrator must intend by their exposure to cause alarm or distress – such that posting nude pictures online without such an intention would not be caught.

6.130 Further, as exposure is already an offence, appropriate sentencing legislation is already in place. Under paragraph 33 of Schedule 3 SOA 2003, Sexual Harm Prevention Orders can be made in respect of the offence of exposure:

(1) where the offender was under 18, he is or has been sentenced in respect of the offence to imprisonment for a term of at least 12 months;

(2) in any other case—

(a) the victim was under 18, or

(b) the offender, in respect of the offence or finding, is or has been

(i) sentenced to a term of imprisonment,

(ii) detained in a hospital, or

(iii) made the subject of a community sentence of at least 12 months.

6.131 If, therefore, the offence under section 66 SOA 2003 were amended to make clear that it includes cyber-flashing, then Sexual Harm Prevention Orders could, in the prescribed circumstances, be made in respect of this conduct. This would provide additional, appropriate protection against cyber-flashing, reflecting the sexual nature of the conduct.

6.132 We therefore propose that section 66 SOA 2003 should be amended to include explicitly the sending of images or video recordings of one's genitals.

**Consultation Question 24.**

6.133 We provisionally propose that section 66 of the Sexual Offences Act 2003 should be amended to include explicitly the sending of images or video recordings of one's genitals. Do consultees agree?

### Scope for a new offence

6.134 Section 66 SOA 2003 was an offence drafted with a particular context in mind. Parliament could not have anticipated the manner or scale of technological change that has now facilitated acts of harmful exposure. It is therefore worth considering whether section 66 is the right vehicle for a cyber-flashing offence, or whether there should be a new offence directed specifically at cyber-flashing.

6.135 There are two limitations in the existing offence that are entirely sensible in cases of live flashing. The question we need to consider is whether those limitations pose an unjustifiable obstacle to prosecution in cases of cyber-flashing, or whether they justifiably narrow the scope of what may otherwise be a very broad offence. The first relates to a conduct element of the offence: the exposure must be of one's own genitals. The second relates to a mental or fault element: the perpetrator must intend

by his or her exposure to cause alarm or distress to those who witness it. We deal with each limitation in turn.

### The conduct element

6.136 The proposition that the exposure must have been of the person's own genitals is, in the context of live flashing, so self-evident as to be barely worth stating. If a person exposes someone else's genitals in the street, that person may be guilty of an offence (perhaps of sexual assault or of encouraging or assisting the offence of exposure, depending on the consent or intention of the other), but it would seem odd for that person to be guilty of an offence of exposure, or to describe them as a "flasher".

6.137 Further, there is seldom any doubt as to whom the genitals belong. If a person exposes themselves in the street, or broadcasts live, that the genitals are those of the person exposing them is generally unequivocal.

6.138 These factors do not so obviously apply in the case of cyber-flashing. A recipient of the image may have no reason to consider that the genitals depicted in the image are those of anyone other than the sender, and the harm suffered by the recipient may be identical regardless.

6.139 It does not necessarily follow, however, that images of another should be brought within scope of this offence. To do so would broaden the scope of the offence significantly and encompass behaviours that, in one sense at least, are quite different. For example, sending a publicly available image of a naked person (that includes their genitalia) to an acquaintance (who knows that the image is not of the sender) would seem to be a different order of threat from that posed by a stranger sending the same image, or where it wasn't otherwise clear that the sender was not the person in the image. (For the avoidance of doubt, this is not to say that the former act would be harm*less*).

6.140 This would seem to suggest that the harm is not merely a function of whether it was the sender's genitalia, but instead a more nuanced question of context and the apprehension of the recipient. Sending someone unwanted pornographic images may be harmful akin to forms of sexual harassment, but this is not to say that such behaviours should be governed by a law primarily focused on exposure.

6.141 Finally, it is worth recalling that this behaviour will be caught under our proposed harm-based offence to the extent that it is likely to cause serious emotional distress.

6.142 Nonetheless, we welcome consultees' views on whether there is a need for an alternative offence based on non-consensual sending of explicit images of a third party (not the sender or the recipient) to deal with this form of image-based abuse.

**Consultation Question 25.**

6.143 Assuming that section 66 of the Sexual Offences Act 2003 is amended to include explicitly the sending of images or video recordings of one's genitals, should there be an additional cyber-flashing offence, where the conduct element includes sending images or video recordings of the genitals of another?

### The mental or fault element

6.144 One of the mental or fault elements in section 66 – intending to cause alarm or distress – is quite restrictive in the case of cyber-flashing. The intention underlying someone's decision to send an exposing image may not necessarily be to cause alarm or distress, yet the harmful impact may be identical nonetheless. To return to the example of an image being sent via AirDrop by one stranger to another on a train, the motive will most likely be entirely unknown to the recipient. But this in no way diminishes the nature of the threat and harm suffered. That this mental or fault requirement is intention to cause alarm or distress, rather than awareness of the risk of causing alarm or distress, further restricts the applicability of the offence.

6.145 We would welcome consultees' views on whether and how this mental or fault element of the offence could be expanded beyond intention to cause alarm or distress. Further, we would welcome views on whether the defendant's awareness of a risk of causing harm (whether alarm or distress, or otherwise) would suffice.

6.146 Professor Clare McGlynn and Dr Kelly Johnson have told us that the offence is characterised by non-consent, and alerted us to, amongst others, the Texan law which requires "express consent".[477]

6.147 However, the mere fact of non-consent alone does not lead inexorably to identical harm. For example, a person in a loving relationship may send an image of their genitalia to their partner; in the context (perhaps the partner was at work) there was no consent to this image (certainly there was no express consent before the fact). Whatever the harm that might attend to this example (and we do not rule out the possibility), it would seem not to cross the threshold of criminality. In any case, the level of harm would seem to be different from the example of the stranger on a train.

6.148 Further, combined with reform to the conduct element, this would become an offence that encompasses behaviours and harms that are very different. The person sending a publicly available nude to a friend without their consent (and where it was clear that the image was not of the sender) would be guilty of the same sexual offence as the person sending images of their own genitalia to strangers. We have real concerns that an offence framed in this way would be overly broad.

[477] Section 21.19(b)(2) of the Penal Code of Texas.

6.149 We therefore consider that cyber-flashing – in the sense of intentional self-exposure to another coupled with some additional mental or fault element – is best addressed under section 66 or its equivalent as a form of unlawful exposure.

**Consultation Question 26.**

6.150 Assuming that section 66 of the Sexual Offences Act 2003 is amended to include explicitly the intentional sending of images or video recordings of one's genitals, should there be an additional cyber-flashing offence, where a mental or fault element includes other intended consequences or motivations, beyond causing alarm or distress?

6.151 Further, should the defendant's awareness of the risk of causing harm (whether alarm or distress, or otherwise) be sufficient to establish this mental or fault element of the cyber-flashing offence?

## GLORIFICATION OF VIOLENT CRIME

6.152 As we explain in the Scoping Report, there are already a variety of inchoate offences that cover inciting, encouraging, aiding, or abetting violent crime.[478] However, some stakeholders, such as law enforcement agencies,[479] have indicated that there may be a need for a broader and more general offence to address "glorifying" violence or violent crime, especially in an online context. In this section, we outline some of the behaviours that might be described as "glorification" of violence or violent crime. Next, we consider the application of the existing law. Finally, we consider whether there is sufficient justification for a specific offence of "glorifying" violence or violent crime.

### "Glorification" of violent crime online: behaviour and impacts

6.153 There are various online phenomena which may be, or have been, described as "glorification of violent crime". One example is drill music – "a genre of rap music that has proliferated in London since the mid-late 2010s"[480] – and drill music videos posted on sites like YouTube. For example, in 2018, five London gang members were given Criminal Behaviour Orders,[481] requiring them not to make "drill music". Detective Chief Superintendent Kevin Southworth said, "We believe this to be one of the first times, if not the first time, we have succeeded in gaining Criminal Behaviour Orders that take

---

478 Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, Chapter 12.

479 See, for example, K Rawlinson, *Police may prosecute those who post videos glorifying violence* (30 May 2018), https://www.theguardian.com/uk-news/2018/may/30/police-prosecute-videos-glorifying-violence (last visited 9 September 2020).

480 J Ilan, 'Digital Street Culture Decoded: Why Criminalizing Drill Music Is Street Illiterate and Counterproductive' (2020) British Journal of Criminology, No 4, pp 994-1013.

481 Introduced by the Anti-social Behaviour, Crime and Policing Act 2014, Part 2.

such detailed and firm measures to restrict the actions of a gang who blatantly glorified violence through the music they created".[482]

6.154 However, some research suggests that the association of drill music with the glorification of physical violence is misguided. For example, in a recent paper, Ilan develops the concept of "street illiteracy" to explain how "British authorities (police, courts and local authorities) misread drill and as a result act in a manner that is counterproductive to crime control."[483] The view that drill music glorifies violence, in Ilan's view, "ignores the ambiguity, braggadocio and fact-fiction hybridity that are characteristic of the genre". Ilan's view is part of a broader concern that drill music represents, rather than endorses, violent crime and, moreover, that creating drill music is a route out of a criminal lifestyle, rather than something worthy of criminalisation.

6.155 The term "glorification of violence" has also been applied recently in the context of death of George Floyd – a 46-year-old black man who died while being arrested in the US city of Minneapolis, Minnesota when a police officer knelt on his neck[484] – and subsequent protests. A Tweet by President Donald Trump, in which he suggested that people looting in the wake of George Floyd's death would be shot, was found by Twitter to violate the platform's rules against glorifying violence.[485] It is noteworthy that this definition of "glorification" includes something more akin to a threat rather than simple praise of violence, suggesting variance and ambiguity in the definition of the term.

6.156 Another example of behaviour that might be described as "glorification" of violence or violent crime is so-called "happy slapping". "Happy slapping" has been defined as the practice of attacking an unsuspecting passer-by and filming it with a camera phone, footage of which is then circulated for the amusement of others. This practice seems to have been most prevalent around 2005 to 2010. While early reports of "happy slapping" involved low level attacks – literally, slapping – this later escalated into very serious violence, sometimes resulting in death. A key aspect of this phenomenon,

---

482 M Holden and S Addison, *London gang ordered not to make 'drill' music glorifying violence (*15 June 2018), available at https://www.reuters.com/article/us-britain-crime-music/london-gang-ordered-not-to-make-drill-music-glorifying-violence-idUSKBN1JB213?feedType=RSS&feedName=lifestyleMolt (last visited 9 September 2020).

483 J Ilan, 'Digital Street Culture Decoded: Why Criminalizing Drill Music Is Street Illiterate and Counterproductive' (2020) British Journal of Criminology, No 4, pp 994-1013.

484 At the time of writing, Derek Chauvin, a former police officer, has been charged with first-degree murder and second-degree manslaughter in relation to George Fletcher's death. See BBC News, *George Floyd death: Ex-officer charged with murder in Minneapolis* (30 May 2020) available at https://www.bbc.co.uk/news/world-us-canada-52854025 (last visited 9 September 2020). See also our discussion in Chapter 4.

485 See, for example, A Hern, Twitter hides Donald Trump tweet for 'glorifying violence' (29 May 2020), available at https://www.theguardian.com/technology/2020/may/29/twitter-hides-donald-trump-tweet-glorifying-violence (last visited 9 September 2020).

aside from the physical violence, is the making and sharing of videos of the attacks, usually accompanied by a message that such behaviour is "funny" or "a joke".[486]

6.157 As we explain in Chapter 4, harms arising from communications can include constitutive harms, direct causal harms, and indirect causal harms. One way to understand "glorification" of violent crime is as conduct adjacent to incitement, where the harmful impact is indirect: "glorification" of violent crime indirectly causes physical violence, through the mediating conduct of others.

6.158 However, "glorification" of violent crime may also involve constitutive and direct causal harms. Constitutive harms may include dehumanising or legitimating violence against an individual or group. Direct causal harms may involve emotional and psychological harm on the part of at least some of those who see the communication. For example, some psychologists have said that the viral sharing of videos of violence against black people can cause "vicarious trauma" those who are exposed to this content, especially other members of the black community.[487]

### Application of the existing law and our proposed harm-based offence

6.159 In the Scoping Report, we noted that music videos encouraging gang violence may be caught by the offences under sections 45 to 46 of the SCA 2007, provided the defendant has done an act capable of encouraging the commission of an offence and he intends to encourage its commission. That the encouragement is general, rather than directed towards an identifiable perpetrator, does not preclude prosecution. Nor does it matter if the intended victim of the physical violence is not an identifiable person.[488]

6.160 However, the offences under the SCA 2007 will not apply to general glorification of violent conduct, where there is no intention or belief that a criminal offence will be committed.

6.161 As we have mentioned above, some content which is considered by the police to "glorify" violence may be the subject of Criminal Behaviour Orders which, if breached, can result in a prison sentence. For example, rappers AM and Skengdo were given a suspended sentence of nine months for breaching the terms of an interim order after they performed drill music and then posted it on social media.[489]

6.162 In addition, some communications "glorifying" violent crime may be caught by the Terrorism Act 2006. The Terrorism Act 2006 uses the definition of "terrorism" in the

---

[486] See, for example, A Harrison, *A Complete History of Happy-Slapping* (26 February 2018), available at https://www.vice.com/en_uk/article/437b9d/a-complete-history-of-happy-slapping (last visited 9 September 2020).

[487] See, for example Matt Zoller Seitz, *The Quiet Trauma of Watching Police Brutality on Our Screens* (09 June 2020), available at https://www.vulture.com/2020/06/police-brutality-footage-vicarious-trauma.html (last visited 9 September 2020).

[488] See the discussion in Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, para 12.88.

[489] See D Hancox, *Skengdo and AM: the drill rappers sentenced for playing their song* (31 January 2019), available at https://www.theguardian.com/music/2019/jan/31/skengdo-and-am-the-drill-rappers-sentenced-for-playing-their-song (last visited 9 September 2020).

Terrorism Act 2000. Under the Terrorism Act 2000, "terrorism" is defined broadly to include "serious violence against a person", as well as "serious property damage", endangerment of another person's life, creating a serious public health or safety risk, and serious interference or disruption to electronic systems.[490] The other aspects of the definition of "terrorism" are that it is the use or threat of action designed to influence a government organisation or intimidate the public; and for the purpose of advancing a political or other similar cause.

6.163 Finally, some communications "glorifying" violence may be caught under our proposed harm-based offence. This is because, as we mentioned above, the harms arising from at least some communications "glorifying" violence include emotional and psychological harms on the part of a likely audience.

**Example 9: glorification of violence causing serious emotional distress**

Freddie sends video clips of a woman being violently attacked to an acquaintance of his, Sara. Both Sara and the woman in the video clips are black. Along with the clips, Freddie sends an accompanying message "Could have been you, Sara! They really got her good." The message includes a string of "thumbs up" emojis.

6.164 Recall that, under existing legislation, "glorification" means any form of praise or celebration.[491] Given that Freddie's accompanying message said, "They really got her good" and included "thumbs up" emojis, his conduct may amount to "glorification" of violence.

6.165 This "glorification" of violence would likely be caught by our proposed offence. A court would probably find that Freddie's communications were likely to cause Sara at least serious emotional distress. Further, the prosecution could probably prove that Freddie intended to cause harm or was aware of a risk of causing harm. There is nothing to suggest that he had a reasonable excuse.

### Is there justification for a specific offence?

6.166 In other jurisdictions, there are offences that criminalise the glorification of violence. These include section 131 of the German Criminal Code. The offence relates to "material which describes cruel or otherwise inhuman acts of violence against humans or humanoid beings in a manner which glorifies or downplays such acts of violence or which represents the cruel or inhuman aspects of the event in a manner which violates human dignity". It does not apply to all forms of communication. It covers only the following:

(1) dissemination or making publicly such material available;

(2) offering, giving, or making such material accessible to a minor;

---

490 Terrorism Act 2000, s 1 and s 2.

491 Terrorism Act 2006, s 20(2).

(3) broadcasting it or making such material available online (for example by streaming) to minors or to the public; or

(4) producing, obtaining, supplying, storing, offering, advertising or importing/exporting for the purpose of dissemination.

6.167 However, we have reservations about creating a broad offence based on "glorification", rather than encouragement of the commission of a criminal offence. An offence based on "glorification" may be incompatible with Article 10 of the European Convention on Human Rights ECHR. Concerns about the combability of "glorification" offences with Article 10 ECHR were raised by the Joint Committee on Human Rights in a report on the Terrorism Bill [492], which later became the Terrorism Act 2006 ("TA 2006"). In the report, criticisms were made of the (proposed) offence of encouragement of terrorism, which includes references to "glorification". In particular, the Committee recommended that "to make the new offence compatible [with Article 10 ECHR], it would be necessary to delete the references to glorification", amongst others measures. This is because Article 10 ECHR requires that any restriction of freedom of expression is clearly prescribed by law:[493] in the Committee's stated view, the term "glorification" is too vague to meet this requirement.[494]

6.168 Despite the concerns of the Joint Committee on Human Rights, the TA 2006 does include references to glorification. Under section 1 TA 2006, it is an offence either to publish a statement or to disseminate a publication that is

> likely to be understood by a reasonable person as a direct or indirect encouragement or other inducement to some or all of the members of the public to whom it is published to the commission, preparation or instigation of acts of terrorism.

6.169 "Indirect encouragement" includes "glorification", which is defined "as including any form of praise or celebration" of acts of terrorism, provided the members of the public could reasonably be expected to infer that "what is being glorified is being glorified as conduct that should be emulated by them".[495] Since the TA 2006 has been passed, its use of the term "glorification" has been criticised by human rights and civil liberties organisations.[496]

6.170 Aside from the vagueness issue, there is a further question about whether a glorification offence is necessary in a democratic society.

---

492 Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters, Report of the Joint Committee on Human Rights (2005-6) HL Paper 75-I, HC 561-I.

493 For full discussion, see Chapter 2.

494 Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters, Report of the Joint Committee on Human Rights (2005-6) HL Paper 75-I, HC 561-I.

495 Terrorism Act 2006, ss 1(3), 20(2).

496 See, for example, Index on Censorship, 'A guide to the legal framework impacting on artistic freedom of expression', available at https://www.indexoncensorship.org/wp-content/uploads/2015/07/Counter-Terrorism_210715.pdf (last visited 9 September 2020).

6.171 It may be that, in the context of terrorism, arguments can be made for unusually stringent restrictions on freedom of expression. For example, when considering the encouragement of terrorism offence under the TA 2006, Eric Barendt noted the relevance of the specific type of conduct to which the glorification, or incitement, or encouragement relates:

> In the leading US case on subversive speech before *Brandenburg*, a plurality of the Supreme Court approved the version of 'clear and present danger' adopted by Learned Hand J in the lower court:
>
> > In each case [courts] must ask whether the gravity of the 'evil', discounted by its improbability, justifies such invasion of free speech as is necessary to avoid the danger.
>
> This is clearly a gloss on the 'clear and present danger' test as formulated by Holmes J, and a gloss which dilutes it considerably. Government can always argue that some dangers are so serious that, even making allowance for their improbability, it is right to suppress all speech which might contribute to bringing them about. The argument is not, however, a silly one, and at times of a real pressing emergency it should be accepted.[497]

6.172 Regardless of the merit of this kind of argument, it cannot, in our view, be made in relation to content "glorifying" violent crime. We have not found convincing evidence to suggest that glorification of violent crime is a "real pressing emergency" that would warrant the significant restriction on freedom expression entailed by a "glorification" offence.

6.173 There is widespread criticism of the existing law under which communications "glorifying" violence may be caught. We have noted above the criticisms of the TA 2006. In addition, following the conviction of AM and Skengdo, a group of 65 people – including representatives from human rights organisations, as well as musicians, lawyers and academics – signed a letter calling on the Metropolitan Police to stop using repressive injunctions against musicians as a means to reduce gang violence.[498] In our provisional conclusion, such criticisms suggest that there is not sufficient justification for a new offence of glorification of violence or of violent crime.

6.174 Finally, we note that there may be alternative options for reform to address broadly this type of conduct. For example, we proposed in 2015 the expansion of the offence of threatening to kill in the Offences Against the Person Act 1861 to include threats to commit violence and threats to rape.[499]

---

497 E Barendt, 'Incitement to, and Glorification of, Terrorism' in I Hare and J Weinstein, *Extreme Speech and Democracy* (2009).

498 Guardian Letters, *Stop criminalising our musicians* (03 February 2019), available at https://www.theguardian.com/law/2019/feb/03/stop-criminalising-our-musicians (last visited 09 September 2020).

499 See Reform of Offences Against the Person (2015) Law Com No 361. These reforms have not yet been implemented.

**Consultation Question 27.**

6.175 Should there be a specific offence of glorification of violence or violent crime? Can consultees provide evidence to support the creation of such offence?

## GLORIFICATION OR ENCOURAGEMENT OF SELF-HARM

6.176 In this section, we explain, first, some of the existing research on online content relating to self-harm, some of which may be considered to "glorify" self-harm. Second, we explain the circumstances under which such content may be caught by the existing law or by our proposed harm-based offence. Finally, we explain why, in our provisional view, there is not sufficient justification for creating a specific offence of "glorification of self-harm".

### Glorification or encouragement of self-harm online: behaviour and impacts

6.177 The literature tends to refer to "non-suicidal self-injury" ("NSSI") content. This may include (but is not limited to) content relating to:

- cutting (which seems to be particularly prevalent),
- disordered eating,
- bruising,
- scratching, or
- substance abuse.[500]

6.178 Research suggests that NSSI content is a "double-edged sword". It can have both positive and negative impacts. One study found four possible benefits as well as three potential risks. The benefits were "mitigation of social isolation, recovery encouragement, emotional self-disclosure, curbing NSSI urges".[501] The risks were "NSSI reinforcement, triggering NSSI urges, stigmatization of NSSI". In another study,

---

500 See, for example, N Shanahan and others, 'Self-harm and social media: thematic analysis of images posted on three social media sites' (2019) 9(2) BMJ Open, available at https://bmjopen.bmj.com/content/9/2/e027006#ref-12 (last visited 9 September 2020).https://bmjopen.bmj.com/content/9/2/e027006#ref-12 (last visited 9 September 2020). See also R Brown and others '#cutting: non-suicidal self-injury (NSSI) on Instagram' (2018) 48(2) Psychological Medicine 337.

501 S P Lewis and Y Seko, 'A Double-Edged Sword: A Review of Benefits and Risks of Online Nonsuicidal Self-Injury Activities' (201) 72(3) Journal of Clinical Psychology 249, available at https://pubmed.ncbi.nlm.nih.gov/26613372/ (last visited 9 September 2020).)..

participants reported that NSSI content can be "both a trigger and a deterrent to NSSI".[502]

6.179 "Glorification" is a vague term. As stated in the section regarding glorification of violent crime, it is defined in the Terrorism Act 2006 as "any form of praise or celebration".[503] Broadly speaking, content "glorifying" violence will involve some kind of positive portrayal thereof. Even under this broad definition, it is not clear how much NSSI content amounts to "glorification" or "encouragement", as opposed to content representing NSSI without endorsement. For example, researchers from the University of Leeds conducted a visual content and thematic analysis of a sample of 602 images captured from Twitter, Instagram, and Tumblr and tagged as "self-harm", one of the aims of which was to identify the extent of positive portrayal of NSSI in social media. They looked for positive portrayal in three different categories:

(1) text included as part of an image, that commented on self-harm as in some way pleasurable, desirable, or attractive;

(2) text included as part of an image, that expressly encouraged viewers to consider or to try self-harm; and

(3) images without text, where a direct representation of self-harm (eg, a wound or a picture of somebody cutting) could be viewed as indicating a degree of glamour or desirability, or alternatively as being attractively transgressive.[504]

6.180 The research found that positive portrayals were far and few between:

> Our findings suggest that clinicians should not be overly anxious about what is being posted about self-harm on social media. Although we found a very few posts suggesting self-injury was attractive, there were no posts that could be viewed as actively encouraging others to self-harm.[505]

6.181 Moreover, this research suggests that NSSI content tends not to be maliciously motivated. Instead, the research found that found that "sharing feelings was a common reason for posting, typically to communicate the distress experienced by the poster."[506] They explain further that:

---

502 Y Seko and others, 'On the Creative Edge: Exploring Motivations for Creating Non-Suicidal Self-Injury Content Online' (2015) 25(10) Qualitative Health Research 1334, available at https://pubmed.ncbi.nlm.nih.gov/25662942/ (last visited 09 September 2020).

503 Terrorism Act 2006, s 20(2).

504 N Shanahan and others, 'Self-harm and social media: thematic analysis of images posted on three social media sites' (2019) 9(2) BMJ Open, available at https://bmjopen.bmj.com/content/9/2/e027006#ref-12 (last visited 09 September 2020).

505 N Shanahan and others, 'Self-harm and social media: thematic analysis of images posted on three social media sites' (2019) 9(2) BMJ Open, available at https://bmjopen.bmj.com/content/9/2/e027006#ref-12 (last visited 09 September 2020).

506 N Shanahan and others, 'Self-harm and social media: thematic analysis of images posted on three social media sites' (2019) 9(2) BMJ Open, available at https://bmjopen.bmj.com/content/9/2/e027006#ref-12 (last visited 09 September 2020).

> Identifying stated purpose and tone was difficult as often images were ambiguous. Nonetheless representations of distress were clear across all sites. Commonly images were posted to provide an understanding about the distress that was being experienced by the poster (213, 35%). There were other messages in the images, such as to inform others, reach out and share recovery (46, 8%). Sadness was the most easily identifiable emotional tone; anger, hope, loneliness and feeling overwhelmed were also identified.[507]

6.182 This is not to say that there is no content that actively encourages acts self-harm. As we noted in Chapter 3, examples of deliberate and malicious encouragement of self-harm include the so-called "Blue Whale Challenge": an online "suicide game" which sets daily "challenges" for "players". Daily "challenges" start with, for example, "wake up in the middle of the night", then escalate to "cut a blue whale into your arm", and finally, to suicide. However, the research does suggest that this kind of content is a small proportion of the overall volume of NSSI content on social media.

### Application of the existing law and our proposed harm-based offence

6.183 We noted in the Scoping Report that, while encouraging or assisting suicide is a specific offence, criminalised under sections 2 and 2A of the Suicide Act 1961, encouraging or assisting self-harm is not. In addition, since there is no specific offence of self-harm, some commentators, such as Gillespie, have written that encouraging self-harm is ostensibly not an inchoate offence under the Serious Crime Act 2007, ("SCA 2007") either.[508]

6.184 However, in the Scoping Report we observed that encouraging potential self-harm may, in fact, be an inchoate offence by virtue of the SCA 2007 and the Offences Against the Person Act 1861 ("OAPA 1861").

6.185 There is an (untested) argument that the offence of intentionally causing grievous bodily harm, or wounding, contrary to section 18 OAPA 1861, could apply to self-harm and therefore could be used in this context. As we noted in our 2015 report on Reform of Offences Against the Person, the section 18 offence includes harm caused "to any person". In contrast, the offence under section 20 of the Act includes only harm to "any *other* person". Therefore, it might be inferred that the section 18 offence is intended to apply to the causing of really serious bodily harm to oneself. If that is correct, then, even in the absence of such harm being caused, anyone seeking to assist or encourage such behaviour – whether online or otherwise – could still be guilty of an offence under sections 44, 45, or 46 of the SCA 2007.[509]

6.186 There are two potential drawbacks of this route to prosecuting communications encouraging self-harm. Firstly, it relies on the argument that self-harm, or at least really serious self-harm or wounding, is a crime. Secondly, if such self-harm is a crime, there is an issue as to whether it should be a crime. Consistent with the

---

507 N Shanahan and others, 'Self-harm and social media: thematic analysis of images posted on three social media sites' (2019) 9(2) BMJ Open, available at https://bmjopen.bmj.com/content/9/2/e027006#ref-12 (last visited 09 September 2020).

508 A Gillespie, Cybercrime: Key Issues and Debates (2016) p 200.

509 See Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, para 12.94.

decriminalisation of suicide by way of the Suicide Act 1961, there is a strong argument that self-harm ought not to be criminalised. Social attitudes have shifted away from viewing suicide and self-harm as wrongdoing worthy of criminalisation.

6.187 Furthermore, or alternatively, some forms of content "glorifying" or encouraging self-harm may also be caught by our proposed harm-based offence. For example, communications akin to the "Blue Whale Challenge" – including the earlier, pre-suicide stages of the "challenge" – may be caught. The prosecution would need to prove that the conduct was likely to cause emotional or psychological harm amounting to serious emotional distress. This should be quite straightforward: it should be relatively easy to argue that persuading someone to injure themselves seriously amounts to psychologically harming them.

6.188 Further, in a context like the "Blue Whale Challenge", it is likely that the prosecution will be able to prove the mental element (intention to cause harm or awareness of a risk of harm). Phillip Budeikin, the perpetrator of the "Blue Whale Challenge" who was convicted in Russia of two offences of inciting a child to commit suicide,[510] reportedly described his victims as "biological waste" and said he was "cleansing society". According to the head of the investigation, Anton Breido, "their task was to attract as many children as possible, then figure out those who would be the most affected by psychological manipulation".[511]

6.189 Of course, the conduct of Phillip Budeikin included not only encouragement of self-harm but also of suicide, and this is reflected in his conviction. However, our view is that similarly motivated encouragement of self-harm, falling short of suicide, would, if it took place in England and Wales, be caught by our proposed harm-based offence. Given the gravity of this kind of conduct, it would likely attract the maximum sentence under our proposed offence: 2 years imprisonment.

6.190 Consider also the following example:

**Example 10: self-harm content causing psychological harm**

Joseph runs an Instagram account called "Eat Clean". Joseph's posts on the "Eat Clean" page recommend dangerously low-calorie diets. They also include captions like "No one likes a fat girl" and "Less weight = more dates" and "Why do you think your thin sister is married and you're not? The answer's there when you look in the mirror!".

6.191 Joseph's posts may be caught by our proposed harm-based offence. The prosecution may be able to prove that the posts are likely to cause emotional or psychological

---

510 S Kholyavchuk, *Founder of Online 'Blue Whale' Suicide Group Sentenced* (19 July 2017), available at https://www.themoscowtimes.com/2017/07/19/founder-online-blue-whale-suicide-group-sentenced-a58446 (last visited 09 September 2020).

511 BBC Newsbeat, *Blue whale challenge administrator pleads guilty to inciting suicide* (11 May 2017), available at http://www.bbc.co.uk/newsbeat/article/39882664/blue-whale-challenge-administrator-pleads-guilty-to-inciting-suicide (last visited 09 September 2020).

harm amounting to at least serious emotional distress. Such harms may include, for example, low self-esteem, poor self-image, or body dysmorphia. As we explain in Chapter 4, research suggests that victims may not experience an immediate emotional reaction to abusive online content, but such content can nonetheless have a psychological impact manifesting in unhealthy and damaging behaviour.

6.192 Unlike the majority of NSSI content (described above), in this example it is more likely that Joseph intended to cause harm or was aware of a risk of harm. He is not sharing his own struggles with an eating disorder, or looking for support. Instead, he is actively encouraging a dangerous diet. Moreover, his captions are of such kind that they could be used as evidence of intention to cause harm or awareness of a risk of harm.

6.193 We acknowledge that our proposed offence could, in some cases, catch NSSI content posted by a vulnerable person, provided that person was aware of a risk of harm. In such cases, the defendant will not necessarily be able to avail themselves of the "reasonable excuse" defence: their vulnerability does not automatically furnish them with a *reasonable* excuse. In such cases, prosecution would probably be ruled out by the CPS, on the grounds that it is not in the public interest. The public interest test has been effective in other contexts, such as encouraging or assisting suicide, where there are a significant number of police investigations but vanishingly few prosecutions.[512] Even so, we would welcome consultees' views on any alternative ways to ensure that vulnerable people who post NSSI content are not caught by our proposed harm-based offence.

**Consultation Question 28.**

6.194 Can consultees suggest ways to ensure that vulnerable people who post non-suicide self-harm content will not be caught by our proposed harm-based offence?

### Is there a justification for a specific offence?

6.195 We have particular concerns about a broad offence of "glorification" of self-harm, rather than a narrower offence of encouragement, akin to the offences under the SCA 2007. Many of the concerns we outlined above, in relation to an offence of glorification of violence or violent crime apply here, too.

6.196 Further, there are arguments against the creation of an encouragement offence. First, even if we set aside the possibility of prosecutions that rely on self-harm being a crime under the OAPA 1861, some of this kind of behaviour would be covered by our

[512] From 1 April 2009 up to 31 January 2020, there have been 156 cases referred to the CPS by the police that have been recorded as assisted suicide. Of these 156 cases, 105 were not proceeded with by the CPS and 31 cases were withdrawn by the police. See Crown Prosecution Service, *Assisted Suicide* (last updated 31 January 2020), https://www.cps.gov.uk/publication/assisted-suicide (last visited 9 September 2020). See also Crown Prosecution Service, *Suicide: Policy for Prosecutors in Respect of Cases of Encouraging or Assisting Suicide* (last updated October 2014), https://www.cps.gov.uk/legal-guidance/suicide-policy-prosecutors-respect-cases-encouraging-or-assisting-suicide (last visited 09 September 2020).

proposed harm-based offence. Therefore, there may not be a pressing need for a specific offence, in addition to the proposed harm-based offence.

6.197 Second, we are conscious that, in relation to this specific kind of communication, there is a significant overlap between "victims" and "perpetrators". The aforementioned research suggests that many of those who communicate online about self-harm tend post content about their own practice of and experiences with self-harm. This suggests that it may be more appropriate to treat NSSI content as a public health issue, using strategies other than the criminal law.

6.198 That being said, there may be a case for a narrow offence of encouragement or incitement of self-harm, with a sufficiently robust mental element to rule out the kind of NSSI content shared by vulnerable people for the purposes of self-expression or seeking support.

**Consultation Question 29.**

6.199 Should there be a specific offence of encouragement of self-harm, with a sufficiently robust mental element to exclude content shared by vulnerable people for the purposes of self-expression or seeking support? Can consultees provide evidence to support the creation of such an offence?

## BODY MODIFICATION

6.200 We note that the potential new offences discussed in the preceding two sections – glorification of violent crime and glorification or encouragement of self-harm – would bear on communications relating to body modification.

6.201 The judgment of the Court of Appeal in *R v BM*[513] confirmed that body modification procedures such as ear-removal, nipple-removal, and tongue-splitting can constitute the offence of causing grievous bodily harm with intent contrary to section 18 of the OAPA 1861, regardless of whether they were carried out with consent. This will be the case provided that the procedure in question does not fall within the "medical exception", which would cover, for example, nipple-removal as part of a mastectomy.[514] Following his unsuccessful appeal in *R v BM*, body modification practitioner Brendan McCarthy pleaded guilty to three counts of causing grievous bodily harm with intent and on 21 March 2019 was sentenced to 40 months imprisonment.[515]

---

513 [2018] EWCA Crim 560.

514 For discussion of the medical exception, see P Lewis, The Medical Exception (2012) 65 Current Legal Problems 355.

515 See, on the CPS website, Tattooist convicted of illegal body modifications (12 February 2019, updated following Mr McCarthy's conviction on 21 March 2019), available at https://www.cps.gov.uk/west-midlands/news/tattooist-convicted-illegal-body-modifications (last visited 09 September 2020).

6.202 For our purposes, the significance of the judgment in *BM* is that carrying out body modification procedures (provided they do not fall within the medical exception) can amount to a violent crime; therefore, communications promoting body modification would likely be covered by one or more of the existing inchoate offences of inciting, encouraging, aiding, or abetting violent crime.[516]

6.203 These offences are serious. For example, for the offences of encouraging or assisting an offence under sections 44, 45 and 46 of the SCA 2007, the maximum penalty is (as a general rule) the same as the maximum available on conviction for the relevant "anticipated or reference offence".[517] So, if a communication regarding body modification is found to amount to encouragement of grievous bodily harm with intent, this could, in theory, carry a maximum sentence of life imprisonment (the same as the maximum sentence for the reference offence, that is, causing grievous bodily harm with intent) – though we note that Brendan McCarthy's sentence was significantly lower than this maximum.

6.204 This is our understanding of the position on communications relating to body modification under the existing law. It is not within our Terms of Reference to make proposals in relation to the existing law covering offences against the person (such as causing grievous bodily harm, with or without intent) or the existing inchoate offences.

6.205 Above we consider the possibility of a new offence of glorification of violent crime. Such an offence would also cover body modification content, provided the content amounted to "glorification" (which is defined under Terrorism Act 2006 as "any form of praise or celebration").[518] As we explain above, we have reservations about creating a broad offence based on "glorification" and we do not provisionally propose any such offence. If such an offence were to be created, our provisional view is that it should be less serious than the existing encouragement offences under the SCA 2007: the maximum penalty should be lower than the maximum penalty for the reference offence.

6.206 In addition, to the extent that a communication promotes self-administered body modification, this may be caught by a potential new offence of glorification or encouragement of self-harm, which we discuss above. However, here again, we incline against a glorification offence. We think there may be a stronger argument for an encouragement offence. However, we are concerned that any such offence should not catch vulnerable people – such as people who are suffering from mental health conditions – who share content for the purposes of self-expression or seeking support. This concern equally applies in the case of body modification.

---

516 See above and Abusive and Offensive Online Communications: A Scoping Report (2018) Law Com No 381, para, Chapter 12.

517 Serious Crime Act 2007, s 58(3). "Anticipated or reference offence" means the offence that is encouraged or assisted.

518 Terrorism Act 2006, s 20(2).

**Consultation Question 30.**

6.207 We welcome consultees' views on the implications for body modification content of the possible offences of:

(1) glorification of violence or violent crime; and

(2) glorification or encouragement of self-harm.

# Chapter 7: Consultation Questions

**Consultation Question 1.**

7.1 We provisionally propose that section 127(1) of the Communications Act 2003 and section 1 of the Malicious Communications Act 1988 should be repealed and replaced with a new communications offence according to the model that we propose below. Do consultees agree?

7.2 By way of summary (though we make separate proposals in respect of each of these below), the elements of the provisionally proposed offence are as follows:

(1) The defendant sent or posted a communication that was likely to cause harm to a likely audience;

(2) in sending or posting the communication, the defendant intended to harm, or was aware of a risk of harming, a likely audience; and

(3) the defendant sent or posted the communication without reasonable excuse.

(4) For the purposes of this offence, definitions are as follows:

(a) a communication is a letter, article, or electronic communication;

(b) a likely audience is someone who, at the point at which the communication was sent or posted by the defendant, was likely to see, hear, or otherwise encounter it; and

(c) harm is emotional or psychological harm, amounting to at least serious emotional distress.

(5) When deciding whether the communication was likely to cause harm to a likely audience, the court must have regard to the context in which the communication was sent or posted, including the characteristics of a likely audience.

(6) When deciding whether the defendant had a reasonable excuse for sending or posting the communication, the court must have regard to whether the communication was, or was meant as, a contribution to a matter of public interest.

**Paragraph 5.50**

**Consultation Question 2.**

7.3 We provisionally propose that the offence should cover the sending or posting of any letter, electronic communication, or article (of any description). It should not cover the news media, broadcast media, or cinema. Do consultees agree?

**Paragraph 5.68**

**Consultation Question 3.**

7.4 We provisionally propose that the offence should require that the communication was likely to cause harm to someone likely to see, hear, or otherwise encounter it. Do consultees agree?

**Paragraph 5.82**

**Consultation Question 4.**

7.5 We provisionally propose that the offence should require that the communication was likely to cause harm. It should not require proof of actual harm. Do consultees agree?

**Paragraph 5.91**

**Consultation Question 5.**

7.6 "Harm" for the purposes of the offence should be defined as emotional or psychological harm, amounting to at least serious emotional distress. Do consultees agree?

7.7 If consultees agree that "harm" should be defined as emotional or psychological harm, amounting to at least serious emotional distress, should the offence include a list of factors to indicate what is meant by "serious emotional distress"?

**Paragraph 5.115**

**Consultation Question 6.**

7.8 We provisionally propose that the offence should specify that, when considering whether the communication was likely to cause harm, the court must have regard to the context in which the communication was sent or posted, including the characteristics of a likely audience. Do consultees agree?

**Paragraph 5.130**

**Consultation Question 7.**

7.9 We provisionally propose that the new offence should not include a requirement that the communication was likely to cause harm to a reasonable person in the position of a likely audience. Do consultees agree?

**Paragraph 5.135**

**Consultation Question 8.**

7.10 We provisionally propose that the mental element of the offence should include subjective awareness of a risk of harm, as well as intention to cause harm. Do consultees agree?

**Paragraph 5.148**

**Consultation Question 9.**

7.11 Rather than awareness of a risk of harm, should the mental element instead include awareness of a likelihood of harm?

**Paragraph 5.153**

**Consultation Question 10.**

7.12 Assuming that there would, in either case, be an additional requirement that the defendant sent or posted the communication without reasonable excuse, should there be:

(1) one offence with two, alternative mental elements (intention to cause harm or awareness of a risk of causing harm); or

(2) two offences, one with a mental element of intention to cause harm, which would be triable either-way, and one with a mental element of awareness of a risk of causing harm, which would be a summary only offence?

**Paragraph 5.160**

**Consultation Question 11.**

7.13 We provisionally propose that the offence should include a requirement that the communication was sent or posted without reasonable excuse, applying both where the mental element is intention to cause harm and where the mental element is awareness of a risk of harm. Do consultees agree?

**Paragraph 5.179**

**Consultation Question 12.**

7.14 We provisionally propose that the offence should specify that, when considering whether the communication was sent or posted without reasonable excuse, the court must have regard to whether the communication was or was meant as a contribution to a matter of public interest. Do consultees agree?

**Paragraph 5.189**

**Consultation Question 13.**

7.15 We invite consultees' views as to whether the new offence would be compatible with Article 10 of the European Convention on Human Rights.

**Paragraph 5.190**

**Consultation Question 14.**

7.16 We invite consultees' views as to whether the new offence would be compatible with Article 8 of the European Convention on Human Rights.

**Paragraph 5.205**

**Consultation Question 15.**

7.17 In addition to our proposed new communications offence, should there be a specific offence covering threatening communications?

**Paragraph 5.211**

**Consultation Question 16.**

7.18 Do consultees agree that the offence should not be of extra-territorial application?

**Paragraph 5.215**

**Consultation Question 17.**

7.19 We provisionally propose that section 127(2)(c) should be repealed and replaced with a specific offence to address hoax calls to the emergency services. Do consultees agree?

**Paragraph 6.18**

**Consultation Question 18.**

7.20 We provisionally propose that section 127(2)(a) and (b) of the Communications Act 2003 should be repealed and replaced with a new false communications offence with the following elements:

(1) the defendant sent a communication that he or she knew to be false;

(2) in sending the communication, the defendant intended to cause non-trivial emotional, psychological, or physical harm to a likely audience; and

(3) the defendant sent the communication without reasonable excuse.

(4) For the purposes of this offence, definitions are as follows:

(a) a communication is a letter, electronic communication, or article (of any description); and

(b) a likely audience is someone who, at the point at which the communication was sent by the defendant, was likely to see, hear, or otherwise encounter it.

Do consultees agree?

**Paragraph 6.32**

**Consultation Question 19.**

7.21 We provisionally propose that the conduct element of the false communications offence should be that the defendant sent a false communication, where a communication is a letter, electronic communication, or article (of any description). Do consultees agree?

**Paragraph 6.38**

**Consultation Question 20.**

7.22 We provisionally propose that the mental element of the false communications offence should be:

(1) the defendant knew the communication to be false; and

(2) the defendant, in sending the message, intended to harm a likely audience, where harm is defined as any non-trivial emotional, psychological, or physical harm.

Do consultees agree?

**Paragraph 6.64**

**Consultation Question 21.**

7.23 We provisionally propose that the false communications offence should include a requirement that the communication was sent without reasonable excuse. Do consultees agree?

**Paragraph 6.67**

**Consultation Question 22.**

7.24 Should there be a specific offence of inciting or encouraging group harassment?

**Paragraph 6.99**

**Consultation Question 23.**

7.25 Should there be a specific offence criminalising knowing participation in uncoordinated group ("pile-on") harassment?

**Paragraph 6.105**

**Consultation Question 24.**

7.26 We provisionally propose that section 66 of the Sexual Offences Act 2003 should be amended to include explicitly the sending of images or video recordings of one's genitals. Do consultees agree?

**Paragraph 6.133**

**Consultation Question 25.**

7.27 Assuming that section 66 of the Sexual Offences Act 2003 is amended to include explicitly the sending of images or video recordings of one's genitals, should there be an additional cyber-flashing offence, where the conduct element includes sending images or video recordings of the genitals of another?

**Paragraph 6.143**

**Consultation Question 26.**

7.28 Assuming that section 66 of the Sexual Offences Act 2003 is amended to include explicitly the intentional sending of images or video recordings of one's genitals, should there be an additional cyber-flashing offence, where a mental or fault element includes other intended consequences or motivations, beyond causing alarm or distress?

7.29 Further, should the defendant's awareness of the risk of causing harm (whether alarm or distress, or otherwise) be sufficient to establish this mental or fault element of the cyber-flashing offence?

**Paragraph 6.150**

**Consultation Question 27.**

7.30 Should there be a specific offence of glorification of violence or violent crime? Can consultees provide evidence to support the creation of such offence?

**Paragraph 6.175**

**Consultation Question 28.**

7.31 Can consultees suggest ways to ensure that vulnerable people who post non-suicide self-harm content will not be caught by our proposed harm-based offence?

**Paragraph 6.194**

**Consultation Question 29.**

7.32 Should there be a specific offence of encouragement of self-harm, with a sufficiently robust mental element to exclude content shared by vulnerable people for the purposes of self-expression or seeking support? Can consultees provide evidence to support the creation of such an offence?

**Paragraph 6.199**

**Consultation Question 30.**

7.33 We welcome consultees' views on the implications for body modification content of the possible offences of:

(1) glorification of violence or violent crime; and

(2) glorification or encouragement of self-harm.

**Paragraph 6.207**

# Glossary

**4chan**

4chan is a website to which images and discussion can be posted anonymously by internet users. The website contains a number of sub-categories – or “boards” – such as, notably, the “Politically Incorrect” board and the “Random” board. The website has proved controversial, and has at times been temporarily banned by various internet service providers.

**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.

**AirDrop**

This is an Apple service that allows users to transfer files (including photographs) between Apple devices using a peer-to-peer wireless connection (ie they are not sent over the internet or mobile network).

**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.

**Body dysmorphia**

This is a chronic mental health condition characterised by extreme anxiety or obsession over perceived physical flaws.

**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.

**Cyberbullying**

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

**Cyberflashing**

The term “cyberflashing” is used to refer to a range of behaviours, but mostly commonly involves a man sending an unsolicited picture of his genitals to a woman.

**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.

**Defendant**

The person accused of an offence.

**Dick pic**

Strictly speaking, this is photograph that a person has taken of their penis. The term more commonly relates to these photographs being sent to another or posted publicly.

**Doxing**

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

**Either-way offence**

An offence that can be tried either in the Crown Court or in a magistrates’ court.

**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.

**GIF**

A GIF ("graphics interchange format") is a moving or "animated" digital image that plays back (or "loops") continuously. They are mostly soundless, and can include short clips of video or film as well as cartoons.

**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.

**Hate Crime**

There is no statutory definition of "hate crime". When used as a legal term in England and Wales, "hate crime" refers to two distinct sets of provisions:

Aggravated offences under the Crime and Disorder Act 1998 ("CDA 1998"), which are offences where the defendant demonstrated, or the offence was motivated by racial or religious hostility;

Enhanced sentencing provisions under the Criminal Justice Act 2003 ("CJA 2003"), which apply to offences where the defendant demonstrated, or the offence was motivated by hostility on the grounds of race, religion, sexual orientation, disability or transgender identity.

A different definition is used by the police, Crown Prosecution Service and National Offender Manager Service for the purposes of identifying and flagging hate crime. The focus of this definition is on victim perception:

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.

The term hate crime is sometimes also used to describe "hate speech" offences, such as offences of stirring up hatred under the Public Order Act 1986, and the offence of "indecent or racialist chanting" under the Football (Offences) Act 1991.

**Indictable offence**

An offence triable in the Crown Court (whether or not it can also be tried in a magistrates' court); contrasted with a summary offence.

**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 of things**

According to researchers at University College London, "internet of things" is "an umbrella term that reflects an evolution of different technologies across a whole spectrum of applications. These range from tiny sensors that collect humidity or temperature levels, to gadgets and household appliances such as "smart" fridges or thermostats, to complex systems such as connected and autonomous vehicles. What makes IoT devices unique is their connectivity. It allows different systems to be interlinked, creating an interdependent network with different devices basically "speaking" to each other." See University College London, *Gender and IoT Research Report, The rise of the Internet of Things and implications for technology-facilitated abuse* (November 2018).

**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.

**Non-binary**

An umbrella term for people whose gender identity doesn't sit comfortably with "man" or "woman". It can include people who identify with some aspects of binary gender identities, and others who completely reject binary gender identities. Non-binary people may also identify under the transgender umbrella.

**Offline communication**

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

**Online abuse**

For the purposes of this Consultation Paper, we adopt the following working definition of "online abuse". Online abuse includes but is not limited to: online harassment and stalking; harmful one-off communications, including threats; discriminatory or hateful communications, including misogynistic communications ("online hate"); doxing and outing; impersonation.

**Online communication**

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

**Online hate**

By "online hate" we mean a hostile online communication that targets someone on the basis of an aspect of their identity (including but not limited to protected characteristics). Such communications will not necessarily amount to a hate crime. We note that the College of Policing's *Hate Crime Operational Guidance* (2014), stipulates that police should record "hate incidents" using a perception-based approach. Again, such incidents may not amount to a hate crime.

**Photoshop**

A software application for editing or retouching photographs and images.

**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.

**Protected characteristics**

In the context of hate crime this refers to characteristics that are specified in hate crime laws in England and Wales, namely; race, religion, sexual orientation, disability and transgender status. The term is also sometimes used in the context of the Equality Act 2010, which specifies nine protected characteristics. There is some overlap between the two, but in this Consultation Paper we are referring to the hate crime characteristics unless we specify otherwise.

**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.

**Summary or summary-only offence**

An offence triable only in a magistrates' court; in contrast to an indictable or either-way offence.

**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.

**TikTok**

TikTok is a free social media application that allows users to watch, create and share short videos.

**Tinder**

A location-based online dating 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 person’s skirt 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”).

**VoIP**

“Voice over Internet Protocol” refers to the group of technologies that allow users to speak to each other over an Internet Protocol (such as the internet) rather than over traditional networked telephone services.

**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.

**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.

**YouTube**

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

**Zoom**

Zoom is cloud-based videoconferencing and messaging software that allows for video meetings with multiple participants (up to 1,000 in some cases).

**Zoom bombing**

Unwanted intrusions into Zoom video calls.