COMBATTING ONLINE HARASSMENT AND ABUSE: A LEGAL GUIDE FOR JOURNALISTS IN ENGLAND AND WALES

June 2021

DISCLAIMER: This guide is for educational purposes only. Every situation is different. A person experiencing an online safety threat should listen to their instincts, discuss their concerns with trusted allies and experts in law enforcement or security. This guide is and should not be relied upon as legal advice. Specialist legal advice should be sought based upon the particular circumstances in which it is needed.

Acknowledgements

This guide has been written by **Beth Grossman**, a barrister at Doughty Street Chambers specialising in media law. Strategic input has been provided by **Caoilfhionn Gallagher QC**, a leading expert in international human rights law and the safety of journalists. This guide draws upon her experience of having advised and assisted journalists dealing with online harassment and fearing for their safety.

The guide was commissioned by the **Media Lawyers' Association** (MLA) and the **Department for Digital, Culture, Media and Sport** (DCMS).

The DCMS commissioned this report as part of its commitment to the National Action Plan for Journalists' Safety. However, the guide is entirely independent of the DCMS.

The MLA is an association of in-house media lawyers from newspapers, magazines, book publishers, broadcasters and news agencies. It was formed to promote and protect freedom of expression, and the right to receive and impart information, opinions and ideas. Its members include in-house lawyers from all of the major UK publishers and broadcasters as well as international news organisations.

Our thanks go to Cian Murphy,Sophie Argent, Zoe Norden and John Battle for their assistance with the preparation of this guide.

Contents

I. Introduction

1. A free press that is able to report fearlessly is the hallmark of a democratic society. Threats to that freedom take many forms, from overt censorship, to attempts to silence journalists by threats to their safety, to under-investment in journalism and precarious employment.

2. Threats to journalist safety may take many forms. The "new frontline", as described in a recent UNESCO report[1], is online harassment and abuse. This phenomenon, of online targeting of journalists, has been described as "one of the gravest threats to press freedom."[2] The global picture is bleak: 73% of women respondents to that UNESCO study reported online violence, and aggressive cyber-harassment campaigns against journalists are waged globally, including in democratic countries which have strong traditions of protecting media freedom.[3] Women, LGBTQ and BAME journalists tend to experience online harassment and abuse in its most severe forms. Journalists who cover particular stories can also be more at risk of facing threats to their safety.[4]

3. This global pattern is reflected in the domestic context. In a recent survey of Media Lawyers' Association (MLA) members, conducted for this report and focusing upon UK journalists and media outlets, 92% reported that abuse of journalists had increased, and the two most common forms were online abuse and harassment. Another recent survey, conducted by the National Union of Journalists (NUJ), revealed that 78% of respondents agreed that, for journalists, "abuse and harassment has become normalised and seen as part of the job."[5] There are multiple examples of journalists subjected to extensive online harassment and

---

[1] Posetti, Aboulez, Bontcheva, Harrison, Waisbord: Online violence Against Women Journalists: A Global Snapshot of Incidence and Impacts, UNESCO, 2020, https://en.unesco.org/news/unescos-global-survey-online-violence-against-women-journalists.

[2] Christophe Deloire, Secretary-General, Reporters Without Borders (RSF), 25 July 2018, launching RSF's report, 'Online harassment of journalists: the trolls attack,' https://rsf.org/en/news/rsf-publishes-report-online-harassment-journalists.

[3] See RSF, 'Online harassment of journalists: the trolls attack' (2018), ibid.

[4] See e.g. Gill Phillips, 'How the free press worldwide is under threat,' 28th May 2020, https://www.theguardian.com/media/2020/may/28/how-the-free-press-worldwide-is-under-threat and Juliette Garside and Jonathan Watts, https://www.theguardian.com/environment/2019/jun/17/environment-reporters-facing-harassment-murder-study

[5] NUJ Members Safety Report, November 2020, available at https://www.nuj.org.uk/resource/nuj-safety-report-2020.html.

abuse, which is often misogynistic, sexist or racist.[6]At the same time, an online and social media presence has become ever-more important for journalists, and particularly freelancers, for newsgathering, reporting and generating interest in their work.

4. Online harassment and abuse have had a devastating effect on the mental health and wellbeing of many journalists, as well as physical consequences. Media outlets have reported significant numbers of employees leaving in consequence[7]. All too frequently, this abuse spills over into offline, physical or face-to-face threats. Even when it does not, women report fears for the safety of their families, and frequently resort to publishing without bylines or under pseudonyms, or decide to stop publishing altogether. More than 30% self- censor in consequence[8].

5. Particular features of online harassment and abuse are its cumulative impact, the difficulty in getting away from it when internet-enabled devices are essential parts of modern life and journalistic activity, and the fact that perpetrators are often unknown and appear as a mob.

6. Ultimately, online harassment and abuse is a threat to freedom of expression. It obstructs and hinders journalists, by making them fear for their safety, and directly interfering in their use of online forums for newsgathering and reporting and generating interest in their stories (particularly for freelancers, who sometimes rely on their social media presence for obtaining work). A recent report by Dubravka Simonovic, UN Special Rapporteur on violence against women, its causes and consequences has described the online abuse of women journalists as a direct attack on the ability of women to participate in public life, undermining the exercise of democracy and good governance and creating a democratic deficit[9]. This problem is urgent and not diminishing: one consequence of Covid-19 lockdowns is a global rise in online harassment directed against women[10].

---

[6] See e.g. https://www.nuj.org.uk/resource/nuj-calls-for-coordinated-effort-to-tackle-online-violence-against-women-journalists.html; https://www.voice-online.co.uk/news/uk-news/2021/04/20/black-channel-4-broadcaster-claps-back-at-online-abuse-with-grace/; and https://www.mend.org.uk/the-consequences-of-journalists-being-racially-abused/.

[7] https://www.pressgazette.co.uk/journalists-mental-health-abuse-newsroom/.

[8] Posetti et al (2021), ibid, and see also RSF (2018), ibid.

[9] http://undocs.org/A/HRC/44/52.

[10] https://news.trust.org/item/20210104110922-bqn8t/.

7. It is possible to take legal action to stop abuse and threats against journalists doing their job. There have been recently cases reported of journalists taking action through the courts, including examples which have led to terms of imprisonment and interim stalking bans for those who have threatened journalists.

8. Taking action may be daunting, particularly for freelancers and for those working at smaller publications. The different options are sometimes technically complex or difficult to navigate. There are practical steps which journalists can take right at the start which are likely to significantly improve their prospects of a satisfactory outcome.

9. For all these reasons, the Media Lawyers' Association is publishing this guide to the law around online harassment. The MLA has been asked by the Department for Digital, Culture, Media and Sport to publish this guide following the establishment of the National Committee for the Safety of Journalists, and the publication of the National Action Plan in March 2021. Our aim is to provide a practical guide for journalists, and those who support them, so that they can understand the different options they have for combatting online harassment and abuse, develop a strategy for doing so, and take immediate steps in highly stressful situations.

II. The problem of online harassment

10. This section considers what is online harassment or abuse. In general terms, online harassment and abuse can be described as the use of online platforms to alarm, distress and/or discredit a person or a group. Coming to a definition is problematic in itself. Harassing behaviour is often coded, or only becomes apparent in the wider context of repeated behaviour by one user, or a "pile-on". It may be wholly or partially covert (for example, where it involves surveillance and stalking); and may take place exclusively online or involve physical instances as well. The situation is further complicated by the fact that online discussion and debate tends to be robust and is frequently expressed in personal language. Therefore, rather than focusing on whether conduct which takes place online *is* harassment or abuse, it is more useful to consider the features which tend to indicate harassment or abuse.

11. Harmful behaviour online includes the following:
    - Making explicit threats, e.g. to kill or injure a person, or to discredit or humiliate them;
    - Making implicit threats – sometimes known as "dog- whistling";
    - Sending distressing material, such as doctored images of journalists or explicit pornography;
    - Publishing private or semi-private information ("doxing");
    - Denial of access to an online forum, by mass false reporting of co-ordinated complaints, or "message bombing" an individual's accounts intended to disrupt their ability to use that platform;
    - Cyber-stalking;
    - Online surveillance;
    - Impersonation and identity theft;
    - Cyber-mob attacks;
    - Orchestrated disinformation campaigns;
    - Persistent and/or high volumes of messages;

- Messages which appear to come from different sources, but attack the journalist in very similar terms.

12. A 2021 study found online harassment and abuse against women journalists is particularly common when the reporting concerns politics, law, economics, sport, women's rights and feminism. It tends to be more severe than that faced by men, and is likely to involve rape threats or sexually graphic and offensive images, and threats against family members. As with physical instances of sexual assault and domestic violence, there is often a pattern of victim-blaming[11]. Common characteristics of online harassment against women journalists are the fact that it is networked, it also targets family, sources and audience members, and the attacks are intimate – often being delivered directly to the woman (by email or direct message) at unusual times and involving highly sexualised content[12].

13. Where it is the context rather than the content of the individual message which causes alarm or distress (e.g. persistent messages, or messages which form part of an intermittent "campaign", or messages which seem to "pile on" the journalist where it appears that there is some degree of coordination) online harassment and abuse may be particularly difficult to identify, especially at the outset. The law can, and does, recognise this type of conduct as constituting a breach of the civil or criminal law. If a journalist feels that they might be experiencing this type of harassment, it is important that they start a comprehensive log, containing the information described below.

14. Online harassment and abuse may emanate from particular individuals, or small groups of individuals, who have nothing more than a personal axe to grind, and the means of doing so via a social media or other form of online account. In other cases, the harassment or abuse may in fact emanate from an organisation or nation-state. In practice, it may be difficult for journalists or organisations to tell. Common features of "bot" accounts include a lack of

[11] Posetti, Shabbir, Maynard, Bontcheva, Aboulez, The Chilling: Global Trends in Online Violence Against Women Journalists, 2021, https://en.unesco.org/sites/default/files/the-chilling.pdf.
[12] Posetti, Online Violence: The New Front Line for Women Journalist, 2020, https://www.icfj.org/news/online-violence-new-front-line-women-journalists.

original content, and a hyper-focus on reposting content on a specific issue. "Troll" accounts are usually identifiable by a combination of factors, including:

- Incorrect or inconsistent use of the definite and indefinite articles in speech;
- An inability to phrase a question by changing the word order;
- Focus on specific themes indicating a partisan political narrative (e.g. the Russian annexation of Crimea in 2014)[13].

15. Journalists may find it very alarming to experience a threat emanating outside the jurisdiction, particularly if there appears to be involvement of a nation-state actor, because it may be perceived that there is an increased cyber-security risk, or risk of physical harm. However, the risks will vary according to the particular circumstances of the harassment or abuse: some threats emanating from state actors come from "troll farms" or equivalents who are not going to go any further than causing annoyance, disturbance, alarm and distress.

16. Conversely, a safety threat is not necessarily less severe because it appears to be emanating from one person. Indeed, a person acting alone may be more likely to move from purely online behaviour to physical harassment and abuse. Recent cases mentioned above have appeared to involve individuals acting alone.

17. To assist journalists in identifying whether the conduct they are experiencing might be harassment or abuse, they should consider the following questions, and discuss their concerns with trusted colleagues. These questions are drawn from the resources provided by a number of organisations (set out in Part 7: Useful Resources):

- Does the conduct experienced include explicit threats, with details such as your name, or how the threat will be carried out, or time or location?
- Does the content refer to friends or family members?
- Does the content seem to be related to incidents which have taken place offline?
- Is the conduct repeated?
- Does the conduct involve individuals giving their real names or information?
- Does the conduct involve people you know, or know of?

[13] https://medium.com/dfrlab/trolltracker-how-to-spot-russian-trolls-2f6d3d287eaa.

- Is the conduct concerted / organised ?
- Is the conduct moving from account to account, or platform to platform?
- Does the conduct involve content which might impact upon your privacy or reputation?
- Do you think you are being stalked?
- Do you think you have been hacked?
- Is the content sexual?
- Do you receive messages or alerts very late at night, or early in the morning?
- Do you tend to receive messages when you are in an isolated or vulnerable location?

III. Steps to take

(a) Background

18. Online harassment and abuse is often a problem with many different dimensions, and resolution may well require a multi-faceted approach. Often, once a safety threat is established, it is difficult for the journalist to react to it in the most appropriate way because vital evidence has been lost (for instance); delay also allows the problem to escalate and may increase the psychological impact of the harassment.

19. This section considers what a journalist may do:
    - Before a problem arises;
    - When the problem starts to arise;
    - To stop or manage the problem by themselves ("self help" remedies);
    - When making a complaint to an online forum;
    - When taking legal action.

Later, this guide sets out the legal and industry standards which underlie these steps.

20. **Responsibility for online harassment and abuse rests solely with those who perpetrate, enable and encourage it. No journalist is to blame, nor should they be blamed, for any matter they report on or investigate which leads to harassment or abuse, or whether or not they take any of the steps suggested below.** In reality, the decision to take any step is complex, with both potential advantages and disadvantages, and may involve time, resources or information which is simply not available.

(b) Before a problem arises

21. Journalists may wish to restrict access to personal information available online and regularly audit the information about themselves which is available. Even innocuous personal information may assist perpetrators in carrying out online harassment and abuse, either

because it provides subject matter or it provides routes into the journalist's offline life (for example, locations they regularly visit or where their children go to school). If possible, journalists should consider whether to maintain separate accounts for personal use, to restrict access to personal photographs and other information and to check that family and friends to whom they are linked publicly online do not disclose this information about them. Location data should be turned off wherever possible. Sources such as LinkedIn and Companies House can often contain information which explicitly gives someone's age, or makes their age obvious, or may identify current and former addresses. If the journalist cannot remove the information directly, they should write to the website asking for its removal.

22. Cyber-security is vital for journalists in protecting themselves (and their sources, colleagues, friends and family) from abuse and harassment. This is a much bigger topic than can be summarised usefully in this guide. Journalists should also speak to security advisers with their employer, or (for freelancers) at commissioning media organisations, or, depending on the circumstances, their union.

23. Journalists should identify who they will discuss their concerns with if they think that a problem is arising. In some cases, this may be the legal or security advisers at their employers. Freelancers should ask their commissioning media outlets if support is available. For those working or freelancing for outlets where support is not available, organisations which may be able to help are identified in Part 7.

(c) When a problem arises

Keeping evidence

24. The single most important step a journalist can take is to **start logging and keeping records, including saving offensive messages and screenshotting, if they so much as suspect that what they are experiencing might be harassment or abuse.** It is significantly more difficult to retrieve evidence at a later date than it is to store it at the time.

Early evidence may be vital in later demonstrating a course of conduct, or showing how the conduct has escalated or become troubling.

25. This is clearly easier said than done. A journalist receiving sexually graphic and threatening images may instinctively wish to delete it to minimise their distress; a journalist experiencing the start of a disinformation campaign may wish to ignore it. At the very least, it is recommended that journalists adopt a "screenshot and file" approach. The original messages should also be kept where possible. It is a good idea to keep a folder in a phone, and/or in an email account, so that relevant saved messages or screenshots can be found quickly in an emergency and kept separate from other messages and activity. Keeping separate folders reduces the extent to which you will be confronted with the distressing material while going about your daily life, and will hopefully reduce the distress caused.

26. If it is possible to keep a fuller evidence log, this will have a number of benefits:

- Identifying relevant features of the conduct, and any patterns in the conduct which make it disturbing (particularly if it takes place across multiple forums or includes offline incident);
- Reassuring the individual that they are not inventing or exaggerating the problem;
- Creating a systematic record which makes it easier to communicate the harassment, or abuse to a third party, whether a trusted ally, employer, online forum, police officer, lawyer, or a court;
- Providing a contemporaneous record for an online forum, or for law enforcement, to help prove the case;
- Making any subsequent complaint to an online platform or the police less time consuming.

27. A log should be kept, and updated during or as soon as possible after each incident, including the following information[14]:

- Date;
- Time;

[14] See https://www.suzylamplugh.org/Pages/FAQs/Category/stalking https://onlineharassmentfieldmanual.pen.org/documenting-online-harassment/.

- Location (if available);
- Nature of incident;
- Form of electronic communication;
- Impact on victim;
- Screenshot of the message (or photograph from a different device if a disappearing message);
- IP information if possible to obtain[15];
- Details of any relevant accounts with which abusive accounts are engaging;
- Details of any offline incidents involving safety threats, including any details or suspicions as to how these might be linked to online threats;
- If the threat is perceived to be escalating, any fact or reason which goes to this;
- If an incident or series of incidents is perceived to be related to the fact of the journalist being a woman, LGBTQ, BAME, disabled, etc, any fact or reason which goes to this.

28. Keeping a log may require a significant time commitment and this may not be feasible in all cases given professional and other personal pressures. Even **if it is not possible to make a full record of every single incident, journalists should try to make a quick note wherever possible.** Often that note will be enough to enable the journalist to recall further details later.

Sharing information

29. Journalists working for the same outlet, or for different outlets, may experience threats which emanate from the same source or sources. Keeping detailed accounts of instances of harassment and abuse, and a better assessment of the level of threat assessed. It may be appropriate to report it to the appropriate individual in your organisation who deals with safety issues which may help assess the level of threat. If there is evidence of multiple and systematic attacks, it is likely to become easier to persuade online platforms, law enforcement agencies and international bodies to take action.

[15] See https://aruljohn.com/info/howtofindipaddress/.

30. It may be advisable to ask a named contact at the online forum, in the police, or any other body handling the issue, to keep a log for future threat assessment and reference.

(d) **Self-help remedies for journalists**

Blocking and muting harassing and abusive accounts

31. In some cases, blocking, muting or restricting the ability of an account to comment or reply can work by starving the abuser (or abusers) of the oxygen of reaction and publicity. These steps also operate to create a barrier and may reduce the level of distress experienced.

32. Blocking or muting an account is an important preliminary step before engaging with the police or the courts. The court is likely to expect any individual making a complaint about persistent harassment which involves messages sent directly to them to have done so and if the individual has not, may well refuse to hold the defendant liable or order an injunction[16]. If a journalist has particular reasons for not blocking or muting, they should record those reasons in their log.

33. Blocking or muting an account might not be sufficient if the perpetrator is seeking to harass the journalist through doxing or degrading content, or wants to engage a wider audience in "piling-on" or if they are likely to create a new account to continue the harassment or abuse. Journalists who are worried about this issue should continue to monitor these accounts, either by asking trusted third parties to do so on their behalf or occasionally "logging out" of their account (e.g. on Twitter) to view what it is being posted.

Redirecting emails

34. Where harassment or abuse comes via email, journalists may wish to consider a "redirect" option either directly to a specific folder, or to a different email account. Redirects can be set up as rules, and be based upon specific email addresses or when emails include specified

16 See *Hayden v Dickenson* [2020] EWHC 3291 and *Scottow v Crown Prosecution Service* [2020] EWHC 3421.

content. A redirect may help to prevent the harassment or abuse causing distress, but the journalist should make sure that the account or folder continues to be monitored, as the information in it may indicate if the harassment or abuse is likely to spill over into physical incidents or escalate in another way.

Engaging with harassment and abuse

35. Some journalists have found that engaging with harassment and abuse - sometimes described as "counter-speech" online, for example by tweeting screenshots of abusive messages, is helpful because it helps to garner support and awareness of the issue and makes the harassment easier to deal with on a personal and professional level. Some believe that this approach is effective because it ends the "normalisation" of online abuse for many perpetrators who are not monsters but "normal people"[17]. Some journalists experiencing online abuse have taken to "naming and shaming" perpetrators by taking screenshots of the abuse which they receive and sharing these online.

36. Although it may be beneficial, engagement is a high-risk strategy. Police advise against direct engagement because it may exacerbate the situation. Journalists should also be aware of the risk that doing so could be used against them:

- By a perpetrator, as the basis of a vexatious complaint or as a defence that what they were doing was "tit for tat" or reasonable in the context;
- By an online platform, as a reason not to remove content, on the basis that messages are not harassing or abusive, but part of a robust conversation;
- By the police or prosecuting authority, as a reason for not investigating or charging, or by the court in making a determination as to whether a defendant is guilty or not guilty, and the reasonableness of any sanction imposed.

37. Journalists who wish to practice counter-speech should:

[17] 'Laws, Norms and Block Bots: A Multifaceted Approach to Combating Online Abuse in Countering Online Abuse of Female Journalists,' OSCE 2016.

- Engage only if there is no physical threat to safety and if they are emotionally prepared to do so;
- Do so strategically and with an end-goal in mind: it is unlikely to change the mind of the person doing the speech but it may help to enlist support or set the record straight;
- Focus on condemning the action rather than criticising the perpetrator;
- Condemn the action by referring to the potential harm which could result;
- Avoid name-calling or insulting language, sarcasm and hyperbole;
- Consider screenshotting and responding generally rather than replying directly to a perpetrator or tagging them in;
- Remove their account information before publishing any screenshot (to avoid counter-allegations of encouraging a pile-on), or keep the account information in for a positive reason, such as alerting other users of the online forum to the dangers of engaging with that account;
- Keeping responses focused on the issue in question, rather than discussions or comments which might be perceived as personal, or which spiral into other subjects;
- Avoid posing questions (or making open-ended comments) as these might be construed as inviting or inciting a response;.

38. The **advantages** of engaging in self-help are that it may stop the problem; it may reduce the distress caused by the harassment or abuse. Even if it isn't successful, it may demonstrate to the tech companies – or the courts – that further action needs to be taken. The **disadvantages** are that these steps might not be enough; there is a risk of loss of evidence from blocking, muting or reporting which can present a problem if the harassment or abuse continues; blocking and muting accounts limits the interactions which a journalist can have online, and many may feel that it limits their potential reach. Online forums, or perpetrators, may seek to argue that counter-speech is "tit for tat".

(e) Complaints to online forums

39. If an online forum responds to a complaint, it is most likely to delete the account or the specific content in question. **It is important to screenshot and log the incident before a report is made**. It is also important to log the fact that a report has been made – again this may be done by screenshot if time is short.

40. Many journalists and their advisers report faster, and more satisfactory responses from online forums where the journalist (or their employer/representative body) approaches a named (and often senior) contact rather than pursuing the complaint through online and generic reporting mechanisms. If other channels are not available, the press or public relations departments may be helpful.

41. Online forums tend to be less effective at dealing with content which is damaging because it is part of a course of conduct rather than a one-off incident, and content which is coded rather than explicit. In these circumstances, particular consideration should be given to approaching a named contact directly, and providing the relevant contextual information.

42. The advantages of complaining to an online forum is that if successful, it may stop the harassment or abuse at source, and without a need for further emotional, time or financial investment by the journalist or their employer. If the complaint is not successful, however, it may have a detrimental effect on the journalist's wellbeing. Even successful complaints may result in a loss of evidence, or may not be sufficient to deal with users who exploit proxy servers or multiple accounts.

43. A further potential disadvantage of making a complaint is that this may potentially be disclosed to the perpetrator if a sanction is challenged (for example) or the perpetrator makes a subject access request. Individuals making complaints (whether through established routes or named contacts) must make sure that they preserve copies of any complaint made and do not overstate their complaint or make any assertion which they cannot back up. Individuals should also be careful not to include information which might exacerbate the harassment or abuse: if it is essential to do so the complaint should clearly state that this information must not be disclosed to the perpetrator or any third party.

(f) Taking legal action

44. Blocking, muting and reporting harassing and abusive accounts may not be sufficient if:
    - The perpetrator(s) try to evade sanctions by opening new accounts, moving to different platforms or persistently creating content which is "under the radar" (e.g. dog-whistling);
    - The content spills over into offline life, or there are signs that it might (e.g. accounts which use their own names and are persistent, or show an interest in the journalist's offline life);
    - The content is particularly disturbing or distressing, e.g. images of sexual abuse, targeted and specific threats of violence, damage or blackmail;
    - The content or behaviour of multiple harassing accounts appears to be coordinated and suggests that they are operating a campaign of vilification.

45. If a journalist is concerned that police involvement may aggravate the situation, they should:
    - Alert their employer or commissioning media outlet;
    - Raise this in any conversation with the police, so that de-escalation strategies can be adopted and security measures put in place;
    - Audit their personal information available online;
    - Consider temporarily protecting their online presence, such as temporarily closing accounts or making them private;
    - Seek a preventative order.

46. **A journalist should go to the police if they perceive any risk that harassment or abuse may spill over into physical harassment or abuse, or if it has already started to do so.**

47. There are a number of steps journalists can take to maximise the prospects of an effective police investigation or positive charging order:
    - Keep a detailed log, and submit it to the police;
    - Identify a police officer who has been specifically trained in dealing with this issue (employers or commissioning organisations might be able to provide this information);
    - Refer to the National Action Plan in any meeting or discussion with a police officer;

- If a Stalking Protection Order is sought, reference the Home Office 2021 guidance[18];
- Explicitly set out, with reference to the evidence and the log, why it is that the journalist says that the threshold of criminal, as opposed to merely annoying behaviour, is met;
- Identify the orders being sought, or the criminal offences which are engaged and the reasons why;
- Journalists who are female, BAME, LGBTQ or disabled and consider that this may be a feature in the harassment or abuse should also reference the CPS Charging Guidelines[19] and emphasise the importance of taking action in the context of the Crown Prosecution Service (CPS) Violence Against Women and Girls (VAWG) strategy and the relevant UN provisions.[20]

48. If the abuse or harassment is being perpetrated anonymously, journalists may wish to take steps in advance which will assist in any investigation, or encourage the police to take these steps:
    - Obtain IP addresses, if possible, from the routes described above;
    - Apply to the online platform for confirmation of the fact that they hold identifying or potentially identifying information such as the IP or ISP address and request that they disclose it. Online platforms will rarely disclose this information without a court order, but may not contest such an application if it is made. The fact that this information is held, and can be obtained, can then be passed onto the police. Alternatively, a journalist who is legally represented might wish to consider making an application (known as a "Norwich Pharmacal" application) to the High Court directly for disclosure.

49. Except for injunctions against persons unknown under the Protection from Harassment Act 1997, the remedies available will all relate to specific perpetrators. An effective way to use action for a wider deterrent effect may be to publicise it. Journalists may wish to rely on this

18 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/951354/SPOs_statutory_guidance_English_with_changes__002_.pdf.

19 https://www.cps.gov.uk/legal-guidance/homophobic-biphobic-and-transphobic-hate-crime-prosecution-guidance.

20 See https://www.cps.gov.uk/publication/violence-against-women-and-girls.

to send a message about the fact that they take harassment and abuse seriously and it will have consequences. This may be particularly important if an injunction has been obtained on a "persons unknown" basis against anonymous perpetrators. However, if the order in question is interim rather than final, care must be taken to ensure that any publicity does not constitute a contempt of court or jeopardise the outcome of the trial.

50. The **advantage** of taking legal action is that it may provide a final resolution to the harassment or abuse, and public vindication for the journalist who has experienced it. The **disadvantage** is that if the police or courts are not receptive, however, it may be not only disappointing but also distressing. Even when the journalist finds that they are receptive, legal action unfortunately takes a long time to reach a final conclusion and often requires a high level of involvement from the journalist.

IV. International legal standards

(a) The Council of Europe

51. The European Convention on Human Rights (ECHR) provides for:
    - The right to **freedom of expression** under Article 10. This includes the right to receive information as well as to impart it. This is a qualified right, which may be restricted in pursuance of a legitimate aim and only to the extent which is proportionate;
    - The right to **private and family life** under Article 8. This includes the right to physical and psychological integrity. It is also a qualified right;
    - The **right to life** under Article 2;
    - A **prohibition on inhuman and degrading treatment** under Article 3.

52. The ECHR is incorporated into UK law under the Human Rights Act 1998. This means that in the UK, all public authorities, including the police, prosecuting authorities and the courts, must act in a way which is compatible with these rights. Authorities may not interfere with those rights directly. They must also give effect to those rights in carrying out their functions. For example, the police should consider if online harassment is affecting a journalist's ability to report and take that into account as a factor in carrying out an investigation.

53. In particular, public authorities have positive obligations (steps they must take) in relation to Articles 2 and 3. Under Article 2, state authorities have a number of such positive obligations, including a duty to put in place a legal and administrative framework designed to provide effective protection for the right to life[21] and a duty to take preventative operational measures to protect an individual whose life is at risk from the criminal acts of another[22]. Similarly, under Article 3, the criminal law must provide adequate protection against the infliction of inhuman or degrading treatment by other private individuals[23] and the state must

[21] This is known as the 'systems duty.'

[22] This is known as the 'operational duty' or the 'protective duty,' and it was first set out in Osman v UK [1998] ECHR 101.

[23] X and Y v Netherlands 8 EHRR 235.

take reasonable steps to prevent inhuman or degrading treatment if they had or ought to have had knowledge of it[24]. Under both Articles 2 and 3, there is a duty to investigate if the state may be in breach of its obligations. The European Court of Human Rights has found violations of Articles 2 and 3 in a number of cases involving journalists[25].

54. These obligations mean that, as a minimum, the relevant authorities make an initial assessment as to whether a threat points to a real and imminent risk to life, and then (if it does so point), go on to undertake a thorough risk assessment, including consideration of relevant preventative measures which might be put in place. There should be a criminal investigation into any serious, or potentially serious, crime targeted at a journalist. Given the risk of online harassment and abuse spilling over into physical harassment or abuse, the prospect of such a threshold being met should be taken seriously by the authorities.

55. In response to the identification of risks to journalists the Council of Europe's Committee of Ministers adopted a Declaration On the Protection of Journalists and Other Media Actors in 2014[26]. This specifically identified threats to female journalists, and amongst the measures proposed urged member states to fulfil their positive obligations and encouraged them to contribute to international efforts by ensuring that legal frameworks and law-enforcement practices fully accorded with international human rights standards. The implementation of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity was encouraged as "*an urgent and vital necessity*".

56. In 2016, the Committee of Ministers adopted recommendation Cm/Rec (2016) 4. This condemned the alarming and unacceptable level of threats to journalists and provided specific Guidelines.[27] These Guidelines include member states taking "appropriate preventative operational measures", including police protection especially when requested or

---

[24] E v Chief Constable of the Royal Ulster Constabulary [2008] UKHL 66.

[25] For example, Dink v Turkey (unreported) 2668/07, 6102/08, 30079/08, for the failure to take reasonable measures to prevent a risk to life following death threats; Najafli v Azerbaijan (unreported) 2594/07 for the failure to carry out an effective and independent criminal investigation after an assault by police at a demonstration. See https://rm.coe.int/factsheet-on-positive-obligations-14june2018/16808b354b for further information and additional examples.

[26] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168056c5e9d.

[27] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415d9#_ftn1.

voluntary evacuation to a safe place. Measures should be effective and timely and be designed with consideration for gender-specific dangers. The Implementation Guide[28] emphasises the importance of prosecuting and treating criminal offences committed online in the same ways as offences offline. The need for law enforcement officials to have training to better investigate such threats is also identified. Threats to life and physical integrity, including rape threats, should be prioritised for prosecution.

In 2016, the OSCE Representative on Freedom of the Media Report recommended that states recognise that online abuse of women media amounts to a direct attack on freedom of expression and the freedom of the media. In the May 2021 Freedom of the Media Report concerns were again raised about declining online safety, especially for women journalists and the increasing challenges of the online sphere, particularly disinformation and the impact of artificial intelligence. The report indicated that further guidance would be issued later in 2021 to enable states to address these issues.

57. The Council of Europe has established a Platform to promote the safety of journalists. It is intended to gather information about serious concerns to media freedom and journalist safety and to foster early warning mechanisms to enable the Council of Europe to take timely and co-ordinated action and adequate policy responses. The platform enables partner organisations (of which there are currently 14: international NGOs and associations of journalists) to issue alerts.

(b) International law

58. At the international level, journalists' rights to freedom and protection from online harassment are protected in a range of ways, including under the International Covenant on Civil and Political Rights (ICCPR). The ICCPR provides for:

- The **right to freedom of expression** under Article 19;
- The **right to privacy, family life and reputation** under Article 17;
- The **right to life** under Article 6;
- A **prohibition on inhuman and degrading treatment** under Article 7.

[28] https://www.ohchr.org/EN/HRBodies/TBPetitions/Pages/IndividualCommunications.aspx#OPICCPR.

59. There are also multiple international instruments which may be relevant, depending on the circumstances of the online harassment – including, for example, the International Convention on the Elimination of All Forms of Racial Discrimination (1965) (CERD), the Convention on the Rights of Persons with Disabilities (2006) (CRPD), the Universal Declaration of Human Rights (1948) (UDHR) and the Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief (1981). The UK is a signatory to these instruments, which should be taken into account in charging decisions, as discussed Part 6.

60. The 2012 Joint Declaration on Crimes Against Freedom of Expression, recommends that States should ensure that crimes against freedom of expression are subject to independent, speedy and effective investigations and prosecutions through:

    - Sufficient resources and training should be allocated to ensure that investigations into crimes against freedom of expression are thorough, rigorous and effective and that all aspects of such crimes are explored properly;
    - Law enforcement bodies should take all reasonable steps to secure relevant evidence and all witnesses should be questioned with a view to ascertaining the truth;
    - The victims should be involved in the procedure to the extent necessary to safeguard their legitimate interests; this includes giving access to certain parts of the proceedings and to the relevant documents to ensure participation is effective;
    - Investigations should be conducted in a transparent manner, subject to the need to avoid prejudice to the investigation.

61. The UN Security Council has adopted Resolution 2222 (2015) acknowledging the specific risks faced by women journalists, media professionals and associated personnel in the conduct of their work. The UN Human Rights Committee has adopted Resolution 39/6 (2018), urging "*States to do their utmost to prevent violence, intimidation, threats and attacks against journalists and media workers, including by putting in place safe gender-sensitive preventive measures and investigative procedures in order to encourage women journalists to report offline and online attacks against them, and providing adequate support, including psychosocial support, to victims and survivors.*" Resolution

38/7 (2018), calls for gender-sensitive responses to take account of particular forms of online discrimination. (These are just examples of a number of recent Resolutions by UN bodies.)

V. Complaints to online forums: industry standards

(a) Background

62. Each online platform has standards for removal of material and processes for individuals experiencing online harassment and abuse to make complaints. The standards and platforms for the main platforms from which journalists are likely to experience harassment or abuse are set out below.

63. In reality, many journalists find complaints processes to online platforms far from satisfactory, and report inconsistent or extremely slow responses to issues raised.

64. Despite this, it is recommended that journalists do pursue complaints about harmful online content (and complaints about the quality of the platform's response) wherever possible. An online platform cannot take steps to remove, prevent or end harmful content or behaviour unless it is aware of it, and even unsuccessful complaints or unsatisfactory responses can assist in building a bank of evidence to persuade that platform to reconsider its approach. The fact that a complaint has been made may be relevant if subsequently making a complaint to the police or the courts, as it will go to any assertion by the journalist that they found the content harmful and that the problem is sufficiently serious to require further intervention. Journalists must, however, be aware that a successful complaint can result in the deletion of material which may later be important as evidence and can be difficult to recover: this is discussed further in Part 6.

(b) Twitter

65. Twitter prohibits threats of, and the glorification of, violence against individuals and groups, targeted abuse and harassment, and hateful conduct, being promoting violence on the basis of a range of characteristics, such as race, ethnicity, national origin, caste, sexual orientation,

gender, gender identity, religious affiliation, age, disability, or serious disease. Its instructions for reporting abusive behaviour are available here.

66. In terms of general abusive behaviour (i.e. that which does fall within the categories of threatening or glorifying violence or amounting to hateful conduct) Twitter states that it prohibits behaviour that *"harasses or intimidates or is otherwise intended to shame or degrade"*. Its guidance[29] goes on to state:

> *Some Tweets may seem to be abusive when viewed in isolation, but may not be when viewed in the context of a larger conversation. When we review this type of content, it may not be clear whether it is intended to harass an individual, or if it is part of a consensual conversation. To help our teams understand the context of a conversation, we may need to hear directly from the person being targeted, to ensure that we have the information needed prior to taking any enforcement action.*
>
> *We will review and take action against reports of accounts targeting an individual or group of people with any of the following behavior within Tweets or Direct Messages. For accounts engaging in abusive behavior on their profile, please refer to our abusive profile policy. For behavior targeting people based on their race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease, this may be in violation of our hateful conduct policy.*

67. Although this states that context may diminish what would otherwise be, or appear to be, abusive or harassing conduct, the converse is clearly also true.

68. Twitter can take action at the level of an individual tweet or direct message (for example, placing a notice on it, either permanently or pending permanent removal) or at the level of an account (for example, placing an account in read-only mode, verifying ownership if it is believed that owners are operating multiple accounts to evade enforcement or for abuse) or permanent suspension.

[29] Current as of 21st June 2021.

69. Twitter also takes steps to identify and disclose networks of state-linked information operations.

(c) Facebook and Instagram

70. Facebook's community standards also prohibit bullying and harassment. These standards distinguish between public and private figures on the basis of allowing discussion. Attacks which are severe, or directly on the individual in question (for example by tagging them in) are prohibited for public figures, whereas protection goes further, encompassing content intended to degrade or shame, for private individuals. It is possible to report anything from a profile, to a page, to a post or comment on a post.

71. Facebook has also created a guide for journalists to use its products safely. This guide provides an overview of how to report abusive content, block harassers and take other steps.

72. Instagram removes content which is harassing or is repeated and unwanted, but again allows "stronger conversations" around public figures or those with large audiences. It encourages reporting of accounts which are intended to bully and harass.

73. Facebook and Instagram maintain an Oversight Board: this Board will consider appeals from decisions made by either forum, but must come from a person appealing with an active account.

(d) YouTube

74. YouTube prohibits content which contains a threat, or which targets an individual based on a physical attribute or membership of a "protected group" (e.g. women, members of the LGBTQ community, disabled people and BAME people). It has an online reporting tool.

(e) WhatsApp

75. WhatsApp's Terms of Service prohibits harassing, threatening and hateful content. Users can be reported, or reported or blocked. Reporting and blocking deletes all messages sent, so downloads and screenshots are vital.

(f) Medium

76. Medium states that it does not tolerate harassment: users can submit complaints electronically.

(g) Email providers

77. An email will usually indicate the company which provides that email account for use. Most companies, under their terms of service, will have standards under their terms of service under which the account can be suspended if it is seen to violate those standards. If an email account is that of the perpetrator's employer, the journalist should go to that employer with their complaint. In some circumstances, the employer may be vicariously liable for their employee's actions, and any failure to take steps after this has been brought to their attention is likely to increase their exposure to legal risk.

VI. Remedies through the courts

(a) Background

78. Journalists may wish to pursue legal action in order to:

- Seek to prevent the behaviour continuing (by injunction or other types of preventative court order);
- Punish the perpetrators, by imprisonment or other forms of criminal sanction;
- Compensate the journalist for the damage suffered (in the civil courts);
- Provide a public judgment, which can serve to "set the record straight" and act as a deterrent.

79. To assist journalists with these considerations, this section describes the main legislative provisions and relevant policies for charging and prosecuting.

80. The main legislation which perpetrators of online harassment and abuse are or may be prosecuted under are:

- The Protection from Harassment Act 1997;
- S1 Malicious Communications Act 1988;
- S127 Communications Act 2003;
- The Computer Misuse Act 1990 (hacking offences).

81. There is a wider range of common law and statutory offences which may be applicable in different circumstances. Of these, the most likely to be relevant are:

- Public Order Act 1986 (s 4, s4A and s5);
- S16 Offences Against the Person Act 1861;
- S63 Criminal Justice and Immigration Act 2008.

82. Injunctions and other types of preventative orders are available under

- The Protection from Harassment Act 1997;
- The Stalking Protection Act 2019;
- The Anti-Social Behaviour, Crime and Policing Act 2014.

83. Journalists may be reluctant to pursue criminal or civil action because of the time that it will take and the belief that it will not succeed or have little effect. Some report concerns that even if action can be successful against one individual, it may aggravate others who are not bound by a court order. There are practical steps which a journalist can take to reduce the time and stress of making a legal complaint and which improve the likelihood of getting a satisfactory outcome, which are outlined in Part 6. Understanding the different legal routes and requirements under the relevant legislation, as well as any avenues for investigation which the journalist believes the police should explore, or factors which should be taken into account in a charging decision is likely to make discussions with the police or any legal adviser more helpful and productive.

84. A further concern which some journalists have raised is that, as individuals relying on their rights of freedom of expression to go about their work, they are not in a position to restrict this right when exercised by others. A journalist has the same human rights as any member of the public. This includes a right to physical and psychological integrity, which is protected by Article 8 of the European Convention on Human Rights. If the online abuse or harassment is interfering with the journalist's ability to do their job, that is an interference with their personal rights to freedom of expression under Article 10. Article 10 also encompasses the right of the public to receive information. In making any order or reaching any judgment, the courts will engage in a balancing exercise weighing the rights of the different parties.

(b) The Protection from Harassment Act 1997

85. The Protection from Harassment Act 1997 can apply to spoken, written or broadcast communications on any medium (s7) as well as to physical acts, to a combination of communication and physical acts .

86. Under the Act, and according to the relevant case law, harassment is:

- A persistent and deliberate course of unacceptable and oppressive conduct[30], and in most – but not all[31] – cases the courts have held that the conduct must be at the very least objectively likely to cause alarm and distress;
- A course of conduct must involve at least two occasions (s7(3)): the court will look at the totality of what has occurred, rather than each act individually, in deciding whether the threshold for oppressive conduct has been met[32];
- The greater the number of incidents, the smaller the time lag between those incidents and the greater the connection between those incidents, the more likely the courts are to find a course of conduct[33];
- Shorter campaigns are more likely to amount to harassment where these involve very serious allegations or distressing content against the complainant or unwarranted threats.

87. The Protection from Harassment Act 1997 also creates a separate offence of stalking (s2A) for conduct which includes contacting, or attempting to contact a person by any means, publishing material relating or purporting to relate to a person or purporting to originate from them, or monitoring the use of a person of the internet or other forms of electronic communication.

88. A person may be liable both for conduct they have perpetrated directly, and that which they have aided, abetted or encouraged. Defences are available for conduct which was for the purposes of preventing or detecting a crime, pursued under an enactment or law, or which was reasonable in the circumstances (s1(3)).

89. When pursued as a criminal offence, the sanctions which may be imposed include a permanent restraining order and imprisonment. A restraining order may be imposed even

30 Majrowski v Guy's and St Thomas' NHS Trust [2006] UKHL 34 .

31 Gerrard v Eurasian Natural Resources Corp Ltd [2020] EWHC 3241 (QB).

32 Iqbal v Dean Manson Solicitors [2011] IRLR 428.

33 Lau v DPP [2000] 1 F.L.R. 799, R v Patel [2006] EWHC 407 (QB).

where the defendant is acquitted if the court considers it necessary to protect the complainant (s5A).

90. Interim injunctions are available under the Act (as a civil remedy) and provide an important route to preventing harassment prior to a matter being decided at a full trial.

(c) Malicious Communications Act 1988 and the Communications Act 2003

91. S1 of the Malicious Communications Act 1988:

- Prohibits the sending of a message – including an electronic message – which is indecent or grossly offensive, conveys a message which is indecent or grossly offensive or conveys a threat;
- It is an essential element of the offence that the purpose – or one purpose – is to cause distress or anxiety to the recipient or to any other person to whom he intends that it should be communicated;
- If the message conveys a threat, there is a defence available if the person sending was made to reinforce a demand on reasonable grounds, and the person had a reasonable belief that they were doing so.

92. S127 Communications Act 2003:

- Prohibits the sending of a message or "other matter" by a public electronic communications network which is grossly offensive, indecent, obscene or menacing;
- There is no express requirement of intent;
- A prosecution must be brought within three years of the relevant acts, and within six months of evidence of those acts (sufficient as to justify proceedings) coming to the prosecutor's attention.

93. S1 Malicious Communications Act requires that the communication be sent to an individual. This may not necessarily cover material merely posted. By contrast, s127 Communications

Act requires the use of a public electronic communications network: this will usually encompass internet and mobile phone networks widely available to the public[34].

94. Under the Malicious Communications Act, the person found liable can be fined or imprisoned (for up to one year if tried in a magistrates' court or up to two years if tried by a jury). Under the Communications Act, a fine may also be imposed; the maximum prison sentence is six months.

95. Injunctions are not available (either prior to full trial or after a guilty verdict) under either piece of legislation. A journalist who thinks that such an order might be important should ask the police to consider applying for bail conditions restraining the conduct until trial or for an interim or final preventative order as well.

(d) The Computer Misuse Act 1990

96. This creates offences a number of relevant offences for activities which in broad terms would be described as "hacking":

- Under s1, unauthorised access to computer material;
- Under s2, unauthorised access with intent to committing or facilitating further offences;
- Under s3: unauthorised access with intent to impair or recklessness as to impairing the operation of a computer (this also applies in denial of service attacks);
- Under s3ZA: unauthorised acts causing or creating risk of serious damage;
- Under s3A making, supplying or obtaining articles for use in a s1 or s3 or s3ZA offence.

(e) Other legislation

34 Chambers v DPP [2012] EWHC 2157.

97. S4, s4A and s5 Public Order Act 1986 create offences respectively for using threatening or abusive writing or visible representations towards another:

- Under s4, with intent to cause that person to believe that immediate unlawful violence will be used against them or another, or to provoke the immediate use of violence, or whereby that person is likely to believe that violence will be used or likely to be provoked;
- Under s4A, with intent to cause harassment, alarm or distress;
- Under s5 within the hearing or sight of a person likely to be caused alarm and distress.

98. An offence is not committed if both parties are inside "dwellings" at the relevant time (meaning a structure occupied as living accommodation): there is no requirement for both parties to be inside the same dwelling. In reality, this creates a significant difficulty for prosecutions of online harassment and abuse because the prosecution is required to prove that neither party was inside a dwelling when the message was sent or received.

99. A threat to kill is an offence under s16 Offences Against the Person Act 1861. The defendant must intend that the person who hears the threat would fear that it would be carried out. That person need not be certain it would be, and a threat may be conditional, does not need to be immediate, and does not need to be made within the jurisdiction.

100. Where the online harassment concerns sexual images, s63 Criminal Justice and Immigration Act may be engaged, which prohibits "*extreme"* pornography (where the image is of an act likely to result in serious injury to a person's breasts, anus or genitals).

101. Injunctions are not available under these pieces of legislation. A journalist who thinks that such an order might be important should ask the police to consider applying for an interim or final preventative order as well.

(f) Charging and prosecution

102. Under the *Guidelines on prosecuting cases involving communications sent via social media*[35] the CPS will apply a two-stage test:

- In the evidential stage, the prosecutor will consider if there is sufficient evidence that the conduct crosses the ambit of protection afforded for freedom of expression, including unwelcome freedom of expression;
- In the public interest stage, the prosecutor, again taking freedom of expression into account, will consider if prosecution is necessary and proportionate.

103. Particular factors which prosecutors should have regard to include:

- The likelihood of re-offending;
- The age and maturity of the suspect;
- The context of the actions, e.g. whether the victim was serving the public, whether it was part of a coordinated attack, whether they were targeted for reporting a separate offence or by a person convicted of a crime against them or someone close to them;
- Whether the suspect has expressed remorse or taken steps to remove the offending communication, whether the communication was intended for or seen by a wide audience;
- Whether the offence constitutes a hate crime.

104. The Guidelines expressly refer to the CPS's Violence Against Women and Girls Strategy, and provides the example of communications containing images of violence against women being accompanied by text that such violence is acceptable or desirable may well, depending on the context and circumstances, be grossly offensive.
https://www.cps.gov.uk/legal-guidance/violence-against-women-and-girls-guidance

[35] https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media.

105. The Guidelines also expressly refer to hate crime in the context of victims of online harassment who are targeted on the basis of their race, religion, disability, sexual orientation or transgender identity. The Guidelines state that the approach to prosecution is underpinned by a number of UN treaties to which the UK is a party: these include the CERD, CRPD, UDHR and the Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief (1981), as set out in Part 4.

106. In practice, online harassment gives rise to a number of difficulties in charging and prosecution. Police officers may not recognise online harassment as particularly serious, although training is an area identified by the National Action Plan for the Safety of Journalists. Perpetrators are likely to be anonymous or pseudonymous and may have taken steps to make evidence gathering difficult (such as the use of "burner" email accounts containing false or non-identifying information to set up the relevant harassing account). These issues are addressed in Part 3.

For offences under the Computer Misuse Act 1990, the CPS will consider factors such as:

- The financial, reputational, or commercial damage caused to the victim(s);
- The offence was committed with the main purpose of financial gain;
- The level of sophistication used, particularly sophistication used to conceal or disguise identity (including masquerading as another identity to divert suspicion);
- The victim of the offence was vulnerable and has been put in considerable fear or suffered personal attack, damage or disturbance;
- The mental health, maturity and chronological age of the defendant at the time of the offence.

(g) Preventative Orders

107. Preventative orders – sometimes known as "injunctions" (this is sometimes but not always the correct legal terminology) – focus on stopping harmful behaviour which may occur in future, rather than punishing that which has already occurred. In some cases, preventative

orders are available on an "interim" basis, prior to full trial. This can provide a more immediate solution and can be very useful for journalists who are concerned about the ongoing interference in their ability to report.

108. Strictly speaking, preventative orders are civil rather than criminal remedies, but a breach of such an order can result in a criminal sentence, prison sentence for the offender.

S3A Protection from Harassment Act 1997

109. Unlike the other types of preventative order, an injunction under the Protection from Harassment Act 1997 does not require police involvement and can therefore usually be obtained more speedily than other remedies. The requirements for an injunction are summarised below. While it is always beneficial to obtain legal assistance in making an application, it is possible to do so as a litigant in person.

110. A further – and sometimes very significant – advantage of an injunction under the Protection from Harassment Act is that, as an interim injunction, it can be made against "persons unknown". This means that it is possible to obtain an injunction against an entirely anonymous defendant, or against a group of defendants, some of whom are known and some of whom are unknown. (The position is potentially different as regards a final injunction at the end of trial.) A "persons unknown" interim injunction might be of assistance to a journalist who needs to take legal action urgently and before it is practicable to identify the perpetrator, or all the perpetrators. The fact that the courts have agreed that the threshold has been met might be useful in persuading an online platform, law enforcement agency or other body to assist in taking further steps to identify the perpetrators or to shut down the avenues which are being used for harassment or prevent further harassment from taking place.

111. If an interim injunction is breached, the defendant will have committed a criminal offence (being contempt of court) and, depending on the circumstances and severity, receive a prison sentence or financial penalty.

112. The disadvantage is that, because it is a civil rather than a criminal remedy, the costs of the application must be met by the individual seeking it – or their employer or publisher – rather than by the state. (Although it may be possible to recover costs at the end of proceedings from the defendant, if found liable.)

113. An interim injunction under the Protection from Harassment Act 1997 can be obtained for an actual breach of the Act or an apprehended breach. It is therefore not necessary to satisfy the court at this stage that the course of conduct does meet the threshold of oppressive or unreasonable behaviour, only that it is likely to do so, if an order is not made.

114. An application does not require police involvement, and is made by an application notice (an "N244" form) supported by evidence (a witness statement setting out what has happened, with a bundle of evidence, known as an exhibit, which should contain the log, screenshots and any other important documents). Unless there is a good reason, the application should be made on three days' written notice to the defendant. A real risk that the defendant would use notice improperly – for example that it might aggravate the harassment – or the need to make an application urgently will be good reasons not to do so. An urgent or without notice application should contain a proper explanation in the witness evidence and the court will order a return date at which the defendant can seek the discharge or variation of the relevant terms.

115. If an order is being sought against "persons unknown", the application should detail the steps they have taken, and the description of the "persons unknown" must be sufficient to enable the court to make an order which clearly identifies those who fall within it and those who are excluded. It is important that the order will not capture people indiscriminately, or capture those who have not committed a civil wrong. The court will scrutinise the criteria used for "persons unknown" extremely carefully.

116. At the interim stage, the court will consider if on a summary evaluation of the evidence which the applicant has put forward it is more likely than not that the threshold for harassment would be met if the matter were to proceed to full trial.

117. The court will also consider:

- What defences the defendant has , or may seek, to argue;

- Whether any order unfairly limits the defendant's Article 10 rights;
- If appropriate, the terms of an order which will provide the necessary level of restraint whilst maintaining the defendant's Article 10 rights as far as possible (for example, a defendant might be banned from tweeting at a particular journalist or making comments about them, but not commenting generally on the issue which that journalist is reporting on).

118. If applying for an interim injunction, it will be necessary to bring a civil claim at the same time or fairly quickly after the order is made (the court will usually direct this) so that the matter can be decided at a full trial.

Stalking Protection Orders

119. Stalking Protection Orders (SPOs) are available under the Stalking Protection Act 2019, on application by a chief officer of police to a magistrates' court for conduct if it appears that the defendant has carried out acts associated with stalking, that the defendant poses a risk associated with stalking to another person and there is reasonable cause to believe that the order is necessary to protect a person from such a risk (whether or not that person was the victim of the previous acts associated with stalking). "Stalking" is given the same meaning as under the Protection from Harassment Act 1997: conduct which includes contacting, or attempting to contact a person by any means, publishing material relating or purporting to relate to a person or purporting to originate from them, or monitoring the use of a person of the internet or other forms of electronic communication.

120. An SPO is available as an interim measure pending trial as well as a final order after trial, when it can be fixed for a period of at least two years or until further order (s3 and s5).

121. An SPO may be a particularly valuable measure in a media environment, where it is known that a particular individual has previously undertaken acts associated with one journalist, and is likely to transfer that conduct to other journalists.

122. In addition to prohibitions, an SPO may also contain positive requirements imposed upon the defendant, such as a requirement to surrender devices, provide the police with access to social media accounts and to devices, and to sign on at a police station.

123. As an application for an SPO is made by the police, there is no charge involved for the journalist or the organisation seeking the order on their behalf. The need for police involvement may also be a disadvantage, if it is difficult to persuade the police of the need to act, or they are unable to act sufficiently quickly. A further potential difficulty is persuading the police or the magistrates' court – that online harassment or abuse amounts to stalking. Where there are clear indications that the behaviour might "spill over", such as direct threats to engage offline, or an indication that the defendant knows where their target lives, this is likely to be easier.

124. In January 2021, the Home Office issued statutory guidance for the police regarding Stalking Protection Orders. (https://www.gov.uk/government/publications/stalking-protection-act-statutory-guidance-for-the-police) The guidance emphasises that relevant stalking conduct can include online or digitally-enabled conduct (paragraphs 7 and 44). Arrests (if necessary) should be made at the first opportunity without any onus on the victim to ask the police to do so (paragraphs 101 – 105).

<u>The Anti-Social Behaviour, Crime and Policing Act 2014</u>

125. Injunctions, including interim injunctions, are available under this Act (s1 and s7) for "anti-social behaviour" on application by the chief officer of police.

126. This is defined, under s2 as including conduct which has or is likely to cause alarm or distress. Criminal behaviour orders are available under s22 where a person is convicted of an offence (not defined as an offence under this Act), where the court is satisfied beyond reasonable doubt that the offender has engaged in behaviour which has caused or was likely to cause harassment, alarm or distress to a person and that making an order will help prevent such behaviour.

127. These powers are not specifically identified in the CPS Guidelines, but nothing in the legislation prevents their use in relation to conduct involving social media. https://www.cps.gov.uk/legal-guidance/criminal-behaviour-orders

(h) Civil claims under the Protection from Harassment Act 1997

128. In a civil claim under s1 and s3, a perpetrator can be made subject to a permanent injunction, and be required to pay compensation (damages) and legal costs. A breach of a permanent injunction can lead to the defendant being imprisoned for contempt of court.

129. If bringing a civil claim, the claimant will still be required to prove that the conduct complained of was oppressive and unacceptable, and of a type to sustain criminal liability[36], although they will only need to prove that to the civil standard – the balance of probabilities – rather than the criminal standard – beyond reasonable doubt.

130. Claims under the Protection from Harassment Act 1997 can be brought in the High Court or in the County Court. It is possible for a claim to be transferred to the County Court after an interim injunction has been ordered in the High Court. Consideration should be given as to whether it is more appropriate for the claim to proceed under the dedicated Media and Communications List in the High Court, particularly if there are complex arguments about different parties' rights to freedom of expression, or claims against anonymous defendants, or suspected involvement of a nation-state.

(i) Threats emanating from outside the jurisdiction

131. It is increasingly common for journalists based in the UK to receive online threats which emanate from outside the UK. For example, journalists at the BBC Persian Service and Iran

[36] Majrowski, ibid.

International have reported receiving death threats and rape threats for their work from Iranian sources[37].

132. The general rule is that a criminal offence may only be triable inside the jurisdiction where it occurs. A substantial measure of the activities constituting a crime should take place in this jurisdiction[38]. Where online harassment and abuse takes place, the question of where the offence "occurs" may be complicated by the fact that some or all of the perpetrator(s) may be in a different country, and the website or application is likely to be hosted in a different county. The fact that material is targeted at a journalist based in this jurisdiction (and available to others in this jurisdiction,) if communicated in a publicly accessible fashion[39] might be considered sufficient.

133. The CPS's *Cybercrime – prosecution guidance*[40] identifies a range of methods which the police and prosecuting authorities can use in cross-jurisdictional cases, including Letters of Request, Joint Investigation Teams and the Global Prosecutors' E-Crime Network.

134. If a threat is real and serious, and domestic remedies are unavailable (for example a foreign government is refusing to cooperate), a journalist may wish to consider leveraging the engagement of an international body. There are significant complexities and nuances around this area, and advice should always be obtained from specialist lawyers, the National Union of Journalists or civil society organisations experienced in working in this area.

(j) Scotland

135. The main pieces of legislation in Scotland are:

- S8 Prevention from Harassment Act 1997, which as in England and Wales includes harassment by written communications on a minimum of two occasions, and for which a

[37] For more information see https://www.nuj.org.uk/resource/un-highlights-ongoing-targeting-and-harassment-of-uk-based-journalists.html; https://news.un.org/en/story/2020/03/1059251.

[38] R v Smith (Wallace Duncan) [2004] EWCA Crim 631.

[39] R v Sheppard [2010] EWCA Crim 65.

[40] https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.

preventative order, known as an interdict , is also available. Unlike in England, this relates only to the civil law and does not create a criminal offence:

- The common law offence of breach of the peace;
- S127 Communications Act 2003;
- S38 Criminal Justice and Licensing Act (Scotland) 2009, prohibiting threatening or abusive behaviour on two or more occasions;
- S39 Criminal Justice and Licensing Act (Scotland) 2009, prohibiting stalking.

136. The Crown Office & Procurator Fiscal Service has produced guidance on the relevant offences and factors going to charging decisions. This Guidance identifies four main categories for prosecution:

- Communications considered to be a hate crime, domestic abuse or stalking;
- Communications constituting credible threats of violence, property damage or incitement to public disorder;
- Communications which may amount to a breach of a court order or a breach of the criminal law regarding publication of proceedings;
- Communications which do not fall into the above categories but are grossly offensive, indecent or obscene or false and result in adverse consequences.

(k) Northern Ireland

137. The main pieces of legislation are:

- The Protection from Harassment (Northern Ireland) Order 1997 (which does not include the specific stalking offence.
- S127 Communications Act 2003.
- Article 3 Malicious Communications (Northern Ireland) Order 1988.

Up-to-date guidelines equivalent to those available in England, Wales and Scotland are not available.

(h) Complaints to international bodies

138. A number of international bodies have either a formal legal role in considering issues when freedom of expression (or violence against women) are engaged, or may have an influential role. These bodies include the European Court of Human Rights, the Council of Europe, UN special procedures, UNESCO and the Organisation for Security and Co-Operation in Europe. Complaints to these international bodies are normally considered when domestic remedies are exhausted or (in some cases) where action is required beyond domestic intervention and is usually reserved for the most serious cases involving failure. This is a highly complex area and it is recommended that any journalist who thinks that such a route might be necessary seeks advice from specialist lawyers with expertise in international media defence.

VII. Useful resources

Guides for journalists

The Rory Peck Trust provides comprehensive resources for freelance journalists, including guides to digital security, psychological risk and risk assessment templates:
https://rorypecktrust.org/freelance-resources/

Pen America has published a comprehensive field manual for online harassment. This has a US focus, but is relevant to journalists working in the UK and elsewhere:
https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

The Suzy Lamplugh Trust contains comprehensive advice about stalking (with a focus on the UK). It provides tools for lone workers and has a National Stalking Helpline:
https://www.suzylamplugh.org/

The International Press Institute has created the Ontheline Platform for Newsrooms, to share resources and best practice:
https://newsrooms-ontheline.ipi.media/about/

The Committee to Project Journalists has created a safety kit and resource hub, and has an email address for journalists needing further assistance:
https://cpj.org/safety-kit/

It may be possible to find IP addresses for email accounts through:
https://aruljohn.com/info/howtofindipaddress/);

Research and reports

Posetti, Shabbir, Maynard, Bontcheva, Aboulez, The Chilling: Global Trends in Online Violence Against Women Journalists, 2021, https://en.unesco.org/sites/default/files/the-chilling.pdf

Posetti, Aboulez, Bontcheva, Harrison, Waisbord: Online Violence Against Women Journalists: A Global Snapshot of Incidence and Impacts, UNESCO, December 2020, https://en.unesco.org/news/unescos-global-survey-online-violence-against-women-journalists

Posetti, Online Violence: The New Front Line for Women Journalist, 2020, https://www.icfj.org/news/online-violence-new-front-line-women-journalists

Combating Violence Against Women Journalists: Report of the Special Rapporteur on violence against women, its causes and consequences, 2020 https://undocs.org/A/HRC/44/52

Office of the OSCE Representative on Freedom of the Media, Safety of Female Journalists Online, 2019 https://www.osce.org/files/f/documents/2/5/370331_0.pdf

Online Harassment of Journalists: Attack of the Trolls, Reporters Without Borders 2018: https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf

Information hubs:

UNESCO resources on the safety of women journalists:
https://en.unesco.org/themes/safety-journalists/women-journalists/resources

Council of Europe resources on threats to media freedom:
https://www.coe.int/en/web/media-freedom/resources

The Council of Europe Platform:
https://www.coe.int/en/web/media-freedom

Dart Centre for Journalism and Trauma:
https://dartcenter.org/resources/journalists-and-online-harassment

International News Safety Institute:
https://newssafety.org/home/

Resources about law

Legislation in the UK:
www.legislation.gov.uk

Case law:
www.bailii.org

Relevant CPS Charging Guidance
https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media

https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

Home Office Guidance on Stalking Protection Orders:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/951354/SPOs_statutory_guidance_English_with_changes__002_.pdf

Guidance in Scotland
https://www.copfs.gov.uk/media-site/latest-news-from-copfs/926-crown-office-sets-out-social-media-prosecution-policy

The National Action Plan for the Safety of Journalists:
https://www.gov.uk/government/publications/national-action-plan-for-the-safety-of-journalists/national-action-plan-for-the-safety-of-journalists