Check for updates

*Article*

The Journal of Criminal Law

The Journal of Criminal Law
2019, Vol. 83(3) 217–228
© The Author(s) 2019
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0022018319829262
journals.sagepub.com/home/clj
SAGE

# The Protection from Harassment Act 1997: Failures by the Criminal Justice System in a Social Media Age

**Laura Bliss**
Edge Hill University, UK

## Abstract

This article will critically examine how the Protection from Harassment Act 1997 is currently being used to tackle online abuse. The use of the Internet to abuse another is on the increase, with the police receiving increasing reports concerning abuse conducted online. This article will examine the failures by the criminal justice system to adequately apply the Protection from Harassment Act in a technology-based world. It will be put forward that changes are needed within the criminal justice system in order to better protect victims of cyber harassment and cyberstalking.

## Keywords

Protection from Harassment Act 1997, social media, stalking, cyber harassment, cyberstalking

## Introduction

The Protection from Harassment Act 1997 (PHA) was enacted into the UK's legal system by the Conservative Government, to prove to citizens that the state was being tough on crime.[1] This followed concerns being raised that the law was failing to adequately protect victims from so-called stalking behaviour:

> Though the offences under the Public Order Act may provide a sanction against stalkers in some instances, offences under the provisions of sections 4 and 4A would be committed only if the stalker intended his behaviour to cause the victim to believe that immediate violence would be used (section 4) or if harassment, alarm or distress is caused (section 4A). There are problems also in applying other aspects of the criminal law against stalkers. The Malicious Communications Act 1988 requires that the article sent must be indecent or

1. J Gowland, 'Protection from Harassment Act 1997: The "New" Stalking Offences' (2013) 77(5) Journal of Criminal Law 387.

**Corresponding author:**
Laura Bliss, Department of Law and Criminology, Edge Hill University, Ormskirk L39 4QP, UK.
E-mail: blissl@edgehill.ac.uk

> grossly offensive. It must also be proved that the sender's purpose was to cause distress or anxiety. In the situations where stalkers continually send greetings cards, flowers or other unsolicited gifts, such intent cannot be proven. The offence of improper use of a public telecommunication system under the provisions of section 43 of the Telecommunications Act 1984 has apparently been useful in tackling obscene or persistent telephone calls. But this covers only one aspect of stalking behaviour.[2]

In 1975, Evonne Van Heussen found herself at the centre of a campaign of harassment and stalking by another individual for a period of 17 years.[3] For the first three years, she was subjected to silent phone calls, photographs being posted through her door and flowers being left outside her home. During this time, she was unaware of who the perpetrator was. However, one evening in 1978, the man responsible for these behaviours broke into her home, holding her hostage for eight hours, where he attempted to rape and strangle her. Local neighbours heard her screams and alerted the police. Despite, Ms Van Heussen only recognising the man as her lecturer from two lectures she had attended a few years earlier, the police labelled the incident as a domestic issue, resulting in the defendant receiving a caution.[4] The stalking continued for a further 13 years, until 1991 when Ms Van Heussen eventually left the country due to the ongoing harassment she was experiencing.

As a result of cases similar to Evonne Van Heussen's, and lobbying by charities calling for a change in the law,[5] Parliament enacted the PHA in 1997 to try and successfully prosecute against the behaviours experienced by victims of stalking and harassment. The mischief behind the Acts implementation was to protect victims of unwanted continued contact, stalking type behaviours and issues with neighbourhood disputes.[6] However, prior to 2012, stalking and harassment were treated as the same offence under the PHA. Following a government review, stalking was criminalised as a specific criminal offence, being substituted into the Act by s. 111(1) of the Protection of Freedoms Act 2012;[7] though there continues to be issues with the distinction between these two types of behaviours.

## Harassment Versus Stalking

Harassment can be defined as '. . . repeated attempts to impose unwanted communications and contact upon a victim in a manner that could be expected to cause distress or fear in any reasonable person'.[8] Whereas stalking is considered the conduct whereby:

> . . . an individual is fixated and/or obsessed with another. This can be exhibited by a pattern of persistent and repeated contact with, or attempts to contact a particular victim.[9]

Stalking, therefore, covers several behaviours and includes acts such as:

> . . . (a) following a person, . . . (d) monitoring the use by a person of the internet, email or any other form of electronic communication . . . [and] (g) watching or spying on a person.[10]

2. Home Office, *Stalking A Consultation Paper* (Home Office, London 1996), paras 3.4–3.6.
3. <http://www.independent.co.uk/life-style/stalked-for-years-by-a-man-she-met-once-1569160.html> (accessed 4 January 2018).
4. Ibid.
5. For example, the Suzy Lamplugh Trust.
6. HL Deb 24 January 1997, Vol 1, col 917.
7. The Home Office, *The Protection from Harassment Act 1997: Improving Protection for Victims of Stalking* (Home Office, London 2012).
8. The Crown Prosecution Service, *Stalking and Harassment* (HMSO, London 2018).
9. <https://www.gov.uk/government/publications/a-change-to-the-protection-from-harassment-act-1997-introduction-of-two-new-specific-offences-of-stalking> (accessed 28 June 2018).
10. Protection from Harassment Act s. 2A (3).

Under the PHA, there is currently no strict definition of stalking, instead, the law consists of several behaviours, like those above, which can be considered as amounting to the conduct of stalking.[11] The lack of a coherent definition in relation to this type of behaviour has meant that the law has not always been applied adequately when it comes to differentiating between harassment and stalking, this is particularly true in cases where social media has been used to facilitate the offence.[12] The following discussion will outline the two offences of harassment and stalking and their current application in a technology-based world.

## Harassment, A Course of Conduct and Social Media

Section 1 of the PHA forbids the conduct of harassing another person. Under the Act, individuals are prohibited from pursuing ' . . . a course of conduct which amounts to harassment of another, and which [a person] knows or ought to know amounts to harassment of the other'.[13] Section 2 of the PHA makes it a criminal offence to harass another person. For the *actus reus* to be established in the offence, it must be found that the behaviour being complained about amounted to both a course of conduct and harassment. If either of these elements is missing, a course of conduct or behaviour constituting harassment, no criminal liability will be placed on the defendant under the PHA.[14]

A course of conduct is considered contact that occurs on at least two occasions where one person is committing the offence.[15] Where two or more people are involved, the law defines a course of conduct as contact ' . . . on at least one occasion in relation to each of those persons'.[16] A course of conduct has been given a wide definition in law:

> I fully accept that the incidents which need to be proved in relation to harassment need not exceed two incidents, but, as it seems to me, the fewer the occasions and the wider they are spread the less likely it would be that a finding of harassment can reasonably be made.[17]

A minimum requirement has, therefore, been set by Parliament as to when certain behaviours may invoke the PHA. However, in most circumstances, for the criminal justice system to be satisfied that a course of conduct is present in a matter, contact must occur on more than two occasions.[18] Here, the conduct must be close in both time and proximity.[19] This can create problems when harassment is pursued via the use of social media:

11. The Crown Prosecution Service (n 8).
12. Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate, *Living in Fear—The Police and CPS Response to Harassment and Stalking* (HMIC & HMCPSI, London 2017) pp. 52–3.
13. Protection from Harassment Act s. 1(1).
14. The *mens rea* for the offence of harassment is based on the construction of knowledge. Here, it must be proven by the prosecution that the defendant, 'knows or ought to know that the[ir] behaviour would amount to [the] harassment of another' (Protection from Harassment Act 1(1)). This will turn on the reasonable person test, where it must be found that the average person, who in the same position as the defendant, would come to the knowledge or should have come to the knowledge, that their conduct would amount to the harassment of another individual. If both the *actus reus* and *mens rea* of the offence can be found, then the defendant is liable for a breach of s. 1(1) of the Protection from Harassment Act.
15. Protection from Harassment Act s. 7.
16. Protection from Harassment Act s. 7(3)(b).
17. *Lau v Director of Public Prosecutions* [2000] 1 FLR 799 (DC) per Schiemann LJ at para. 15.
18. J Agate and J Ledward, 'Social Media: How the Net Is Closing in on Cyber Bullies' (2013) 24(8) Entertainment Law Review 263, 266. It is important to note that under s. 1(3) of Protection from Harassment Act, there is a defence available with regard to 'a course of conduct': ' . . . (a) that it was pursued for the purpose of preventing or detecting crime, (b) that it was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under any enactment, (c) or that in the particular circumstances the pursuit of the course of conduct was reasonable'.
19. Agate and Ledward (n 18). See also, *Lau v Director of Public Prosecutions* [2000] 1 FLR 799 (DC) per Schiemann LJ at para. 15.

> The requirement that the harassee shows a course of conduct amounting to harassment, with the acts forming that harassment equating to actionable criminal acts makes it difficult for someone suffering the posting of slanderous comments, or the taking over of email addresses, or the bombarding with messages, to obtain legal satisfaction . . . .[20]

The anonymity of the Internet has made it easier for harassment to be conducted[21] and has been coined cyber harassment.[22] However, the ability to fit s. 2 of the PHA to a technology-based world can be difficult when it comes to establishing a course of conduct. In many cases, social media profiles can be created with very few security questions being asked.[23] For example, to create a Facebook profile, the user merely needs an email address; all other questions can be answered using an alias.[24] Consequently, we have witnessed a rise in fake accounts,[25] which can be created solely for the aim of tormenting another individual.

The use of fake online profiles and the anonymity of the Internet can create difficulties for victims and the police in tracking perpetrators of online harassment, further exacerbated if the perpetrator is unknown to the victim,[26] despite a digital trace being available. All electronic communications can be traced to an IP address;[27] however, if a person has used a public network to facilitate abusive behaviour online, it can become impossible in some instances to track the perpetrator,[28] especially if the comments have come from outside of the UK. Here, the justice system must rely on the cooperation of social networking companies, such as that of Facebook and Twitter, who have been reluctant in the past to release information about its users.[29]

For a successful conviction under the PHA, the prosecution must be able to prove a course of conduct that exceeds more than two occasions. Here, each separate complained about behaviour must directly link back to the accused. If a perpetrator of online abuse uses multiple servers, along with fake social media profiles, this can cause issues in establishing a course of conduct, especially in a time when police funding is being reduced.[30]

## Harassment and Social Media

If a course of conduct can be established, next, the complained about behaviour needs to amount to harassment, as governed under s. 1(1) of the PHA. Harassment under the Act includes the behaviours of 'alarming' a person or causing them 'distress'.[31] To prove alarm or distress, this will be essentially an evidential exercise, based on the case facts:

---

20. M Salter and C Bryden, 'I Can See You: Harassment and Stalking on the Internet' (2009) 18(2) Information & Communications Technology Law 99, 100.
21. For example, research conducted by Women's Aid found that 85% of those surveyed had received online abuse by a partner or ex-partner. <https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/> (accessed 9 October 2018).
22. J Brannon, 'Crime and Social Network Sites' (2013) 1 Judicial Review 41, 43.
23. Salter & Bryden (n 20) at 99.
24. <https://www.facebook.com/help/345121355559712> (accessed 12 November 2017).
25. Between January and March 2018, Facebook removed 583 million fake accounts. <http://www.bbc.co.uk/news/technology-44122967> (accessed 17 May 2018).
26. Salter and Bryden (n 20) at 101.
27. An IP address is a unique code which identifies a computer using a communications network.
28. DK Citron, *Hate Crimes in Cyberspace* (Harvard University Press, USA, 2014) 165.
29. <http://www.telegraph.co.uk/technology/twitter/9834776/Twitter-refuses-to-hand-member-information-to-police.html> (accessed 28 June 2018).
30. It is currently estimated that police funding will be reduced by £700 m by 2020. <https://www.theguardian.com/uk-news/2017/nov/09/britains-police-budgets-to-lose-700m-by-2020-amid-rising> (accessed 1 August 2018).
31. Protection from Harassment Act s. 7(2).

> Where the quality of the conduct said to constitute harassment is being examined, courts will have in mind that irritations, annoyances, even a measure of upset, arise at times in everybody's day-to-day dealings with other people. Courts are well able to recognise the boundary between conduct which is unattractive, even unreasonable, and conduct which is oppressive and unacceptable. To cross the boundary from the regrettable to the unacceptable the gravity of the misconduct must be of an order which would sustain criminal liability . . . .[32]

It is clear from previous case law that the matter needs to go beyond what can be deemed as 'disturbing' and 'unpleasant' behaviour, to 'cross [a] boundary' to invoke the criminal law, allowing the criminal justice system to uphold a person's right to freedom of expression.

Under Article 10 of the European Convention on Human Rights, States who are signatory to the Convention must protect a citizen's right to free speech in order to maintain a democratic society.[33] This includes the right to be offensive:

> Freedom of 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.[34]

Despite the need to protect free speech, Akhtar argues that the criminal justice system has 'tilted' too much in the direction of freedom of expression when it comes to matters concerning conduct carried out online.[35]

In a social media age, the high threshold associated with free speech puts further disadvantages on victims of cyber harassment. In many cases, the matter being complained about can be considered as 'disturbing, unpleasant and may transgress the norms of socially acceptable'[36] behaviour, but it is difficult to prove that the conduct crosses the evidential line to be considered as breaching the law. This is further reflected in the work of Basu and Jones, who suggest that conduct carried out via the aid of social media is more sinister than offline behaviours.[37] As a result, the criminal justice system is struggling to appreciate the severity cyber harassment can have upon an individual, shown further in the abuse experienced by Caroline Criado-Perez in 2013.

Ms Criado-Perez, an active feminist supporter, launched a public campaign in 2013 to get the well-known author, Jane Austin, printed on banknotes in the UK. Following her launching the campaign, Ms Criado-Perez was subjected to explicit threats of sexual violence online, including threats of rape. Comments encompassed 'rape her nice ass' and 'fuck off and die you worthless piece of crap'.[38] In particular, one individual, Peter Nunn, tormented her with a crusade of misogynistic abuse, as detailed in Ms Criado-Perez's blog:

> He dug up my work history. He dug up my relationship and family history. He dug up my family's work history—including publishing home addresses. He wrote reams of blogs about me and my every public move. He made numerous videos about me. He set up numerous twitter accounts all of which spoke almost exclusively about me. In these same twitter accounts he detailed the best way to rape and drown a witch, alongside repeatedly naming me as the head of the 'witches' coven'. He also boasted on twitter in the same account about having bought a gun, and wondered 'how much death' this gun could buy him.[39] [sic]

---

32. *Majrowski v Guy's and St Thomas's NHS Trust* [2006] UKHL 34, [2007] 1 AC 224 per Lord Nicolls at para. 30.
33. *Handyside v United Kingdom* (1976)1 EHRR 737 at para. 49.
34. *Redmond-Bate v DPP* [2000] HRLR. 249 per Sedley LJ at para. 20.
35. Z Akhtar, 'Malicious Communications, Media Platforms and Legal Sanctions' (2014) 20(6) Computer and Telecommunications Law Review 179, 181.
36. Salter and Bryden (n 20) at 103.
37. S Basu and R Jones, 'Regulating Cyberstalking' (2007) 2 Journal of Information, Law and Technology 1 at para. 45.
38. <https://www.theguardian.com/society/2014/jan/07/jane-austen-banknote-abusive-tweets-criado-perez> (accessed 10 October 2016).
39. Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate (n 12) at 27.

Despite a clear course of conduct being present, Nunn was prosecuted and found guilty of sending grossly offensive communications contrary to s. 127 of the Communications Act 2003 (CA). He received a six-week custodial sentence.[40]

Ms Criado-Perez has been very critical of the Crown Prosecution Services (CPS) charging decision in the matter of Nunn:

> This man made me fear for my life as no-one ever has before. I felt he was a clear and present threat to me. He made me scared to go outside, to appear in public. He stopped me being able to sleep; being able to work. He seemed obsessed enough to carry out his threats. I am glad he has been found guilty. I am glad he cannot contact me again. I hope he has learnt from this. But I think the CPS got the charge wrong. I don't feel they understood what happened to me.[41]

By applying the *actus reus* of s. 1 of the PHA, it is difficult to distinguish why the case of Nunn was prosecuted under s. 127 of the CA as opposed to the PHA. Nunn contacted her on numerous occasions, clearly fulfilling the elements required for a course of conduct. Furthermore, Ms Criado-Perez was made to fear for her own life, with the behaviour she was subjected to having significant effects on her employment and mental well-being. Yet, the CPS brought an action before the court under a different Act of Parliament, suggesting that the criminal justice system is struggling to appreciate when the PHA can be used to protect victims of online abuse.[42] The case of Nunn illustrates the continued problems the criminal justice system experiences when it comes to labelling an incident as cyber harassment. This is particularly true when it comes to stalking offences and the use of the PHA in a social media context.

## Stalking and Social Media

Whereas s. 2 criminalises the conduct of harassment, s. 2A makes it a specific illegal offence to stalk another person. As previously stated, prior to 2012, stalking and harassment were treated as the same offence and both governed under s. 2 of the PHA. However, in 2012, stalking was included in the Act as a separate offence in its own right under s. 111(1) of the Protection from Freedoms Act, after concerns were raised that the law was failing to protect stalking victims:

> The majority of respondents considered that [the] current legislation [PHA] was inadequate for dealing with stalking perpetrators (56%) and 51% felt that stalking needed to be defined in law through a specific offence.[43]

Under s. 2A of the PHA, it is an offence to pursue '. . . a course of conduct in breach of section 1(1), . . . [in which] the course of conduct amounts to stalking'.[44] Like that of the offence governed under s. 2 of the Act, the *actus reus* consists of a course of conduct that occurs on at least two occasions, where there is one perpetrator, which can be considered as causing alarm or distress upon the victim. In addition, it must be found that the complained about behaviour amounts to stalking under the law. As mentioned previously, the PHA does not contain a specific definition of stalking; instead, the Act encompasses a non-exhaustive list of conducts, which are considered to amount to this type of behaviour:

> The following are examples of acts or omissions which, in particular circumstances, are ones associated with stalking—(a) following a person, (b) contacting, or attempting to contact, a person by any means, (c)

40. *R v Peter Nunn* unreported 29 September 2014 MC.
41. <https://weekwoman.wordpress.com/2014/09/29/a-brief-comment-on-peter-nunn/> (accessed 29 October 2016).
42. Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate (n 12) at 87.
43. The Home Office (n 7) at 14.
44. Protection from Harassment Act s. 2A(1).

> publishing any statement or other material—(i) relating or purporting to relate to a person, or (ii) purporting to originate from a person; (d) monitoring the use by a person of the internet, email or any other form of electronic communication, (e) loitering in any place (whether public or private), (f) interfering with any property in the possession of a person, (g) watching or spying on a person.[45]

If the issues being complained about can be regarded as stalking, and a course of conduct is present in the matter which amounts to harassment, then the *actus reus* for s. 2A of the PHA will be satisfied.[46]

Like that of harassment, it has been accepted that stalking can now be pursued online and is commonly referred to as cyberstalking.[47] However, cyberstalking, similar to stalking itself, lacks a rigid legal definition.[48] Instead, it has been suggested that certain behaviours can be associated with stalking online:

> seeking and compiling information on the victim in order to harass, threaten and intimidate the victim online or off-line; repeated unsolicited e-mailing and Instant Messaging; electronic sabotage such as spamming and sending viruses to the target; identity theft; subscribing the victim to services; purchasing goods and services in the victim's name; impersonating another online; sending or posting hostile material, misinformation and false messages (e.g. to Usenet groups); and, tricking other Internet users into harassing or threatening a victim (e.g. by posting the victim's personal details on a bulletin board along with a controversial invitation).[49]

The Internet has now created new and unique ways to stalk another, while allowing for direct contact between the perpetrator of the offence and the victim, which in many cases can occur 'around the clock'.[50] There continues to be, however, issues as to when someone's continued unwanted contact goes beyond the conduct of harassment to stalking.

This has caused several problems in the criminal justice system, as exposed in a report conducted by the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate in 2017:

> There are many links between harassment and stalking, including the legislation itself. However, we found that the police and the CPS frequently struggled to separate the two offences. We found that stalking in particular was misunderstood by the police and the CPS. As a result, it often went unrecognised. The police sometimes mis-recorded stalking offences, or worse, did not record them at all. Prosecutors on occasions missed opportunities to charge stalking offences, instead preferring other offences, particularly harassment.[51]

The report was conducted following the annual Violence against Women and Girls review in 2016.[52] The 10th anniversary edition found a drop-in prosecutions brought under the PHA. Consequently, a recommendation was put forward to the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate to investigate why fewer matters were being prosecuted contrary to the PHA.[53]

During the investigation, it was found that there was a complete failure across all police forces in England and Wales to take the reporting of harassment and stalking behaviour seriously. In addition,

45. Protection from Harassment Act s. 2A(3).
46. It is important to note that under s. 4A(4) of the Protection from Harassment Act, there is a defence available with regard to a course of conduct amount to stalking: '. . . (a) A's course of conduct was pursued for the purpose of preventing or detecting crime or, (b) A's course of conduct was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under any enactment, or (c) the pursuit of A's course of conduct was reasonable for the protection of A or another or for the protection of A's or another's property'.
47. L Sheridan and T Grant, 'Is Cyberstalking Different?' (2007) 13(6) Psychology, Crime & Law 627–29.
48. The lack of a specific legal definition in relation to cyberstalking is supported by Gillespie. See, AA Gillespie, 'Cyberstalking and the Law: A Response to Neil MacEwan' (2013) 1 Criminal Law Review 38.
49. Sheridan and Grant (n 47) at 627–28.
50. N MacEwan, 'The New Stalking Offences in English Law: Will They Provide Effective Protection from Cyberstalking?' (2012) 10 Criminal Law Review 767, 771.
51. Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate (n 12) at 7.
52. The Crown Prosecution Service, *Violence against Women and Girls report: Tenth Edition* (HMSO, London 2017).
53. Ibid at 7.

112[54] cases of stalking and harassment were examined in detail, with the report concluding that '[n]one of these cases had been dealt with well'.[55] In many of these matters, police forces misunderstood the differences between these two types of behaviours, as harassment and stalking are inherently interlinked.[56]

As previously stated, there is no specific legal definition of stalking, instead, the PHA relies on the idea that the conduct falls within the 'definition of harassment'.[57] However, for MacEwan, this ideal is not possible, as certain behaviours which amount to stalking, 'within a cyberstalking context', may not pass the threshold of harassment to warrant criminalisation, for instance, 'watching and spying on a person'.[58] This is disputed by Gillespie, who suggests that the PHA is flexible enough to be used to prosecute cyberstalking offences:

> The law, it is submitted, can protect victims. The flexibility of a 'course of conduct', and the interpretation the courts have taken to both the victim impact condition and the mens rea element mean that where covert activity is detected it is highly likely that the offence would be established.[59]

Nevertheless, as exposed in the report conducted by the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate, the lack of a coherent definition in relation to stalking, is creating serious misunderstandings in the criminal justice system.[60] This is more evident when social media is used to facilitate the offence, as experienced by Nicola Roberts.

Ms Roberts, a well-known performer from the band, 'Girls Aloud', was subjected to thousands of threatening messages, her social media accounts being used to spy on her and made to fear for her own life, by an ex-partner.[61] He stalked her for a period of 10 years. During this time a restraining order was placed upon her ex-partner, which was later broken when he started 'following' her on the social networking site Instagram. Subsequently, he was charged for breaching his restraining order; however, these charges were later dropped by the CPS:

> The failure in Nicola's [Roberts] case was born out of a lack of understanding about how certain social media platforms work, which resulted in a decision to offer no evidence. Due to how the CPS dealt with this procedurally, no charges can now be brought.[62]

The CPS has since apologised for their lack of understanding 'about how certain social media platforms work'.[63]

## The Criminal Justice System, Social Media and the PHA

The Home Office, in July 2012, undertook a complete review of the PHA, paving the way for stalking to be included as a specific offence under the Act. The information gathered from the study uncovered that 69% of those surveyed (156 people) felt that the criminal justice system did not fully understand stalking. This is even more apparent when the behaviours criminalised under the PHA are conducted online, as reflected in the work of Salter and Bryan:

54. Of these 112 cases, 82 cases involved social media.
55. Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate (n 12) at 13.
56. MacEwan (n 50) at 769.
57. Ibid.
58. Ibid.
59. Gillespie (n 48) at 45.
60. Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate (n 12) at 7.
61. <https://www.independent.co.uk/arts-entertainment/music/news/nicola-roberts-stalker-girls-aloud-cps-apology-carl-davies-a8459656.html?amp&__twitter_impression=true> (accessed 27 July 2018).
62. Ibid.
63. Ibid.

> There is also evidence that the concept of cyber harassment is not always taken seriously, with advice to victims being simply to change their email address or to switch off their computers.[64]

Sadly, a response which is still given by some police forces:

> It wasn't her (the perpetrator's) fault for sending abusive Facebook messages, it was my fault for being on Facebook . . . And the only way to stop these messages is if I deactivate my Facebook account, and come off social media. I didn't think that was very fair at all.[65] [sic]

Victim blaming is not a new phenomenon within the justice system and is often used to reflect the crime onto the person who has reported the offence.[66] For instance, in relation to sexual assaults and rape, victims are often questioned on their choice to walk home alone in the dark.[67] In many cases, victims are even judged on their choice of clothing when the incident occurred.[68] This attitude has now been reflected towards complainants of social media abuse, who are often blamed for their experiences simply for having a social media profile.

The lack of understanding by the criminal justice system in relation to cyber harassment and cyber-stalking is also mirrored in the justice systems approach to cybercrime in general.[69] In 2012, an individual had his conviction for the sending of malicious communications under s. 127 of the CA overturned by the High Court, after it was concluded that a message he had sent on Twitter was indeed an 'ill-thought out-joke' as opposed to a criminal offence.[70] Paul Chambers, following the closure of Doncaster Robin Hood Airport, took to Twitter to vent his frustration at not being able to fly to Northern Ireland to meet with his girlfriend: 'Crap! Robin Hood Airport is closed. You've [sic] got week and a bit to get your shit together otherwise I'm blowing the airport sky high'. At the court of first instance, he was convicted and fined £385, along with being ordered to pay £600 in court fees. Following this case, and others,[71] guidelines were created for matters concerning conduct carried out online via the use of social media.

The guidelines were made publicly available in 2013, later being updated in 2016 and 2018. The purpose of the guidelines was to 'give clear advice to prosecutors who have been asked either for a charging decision or for early advice to the police . . . '.[72] This was advocated by the then Director of Public Prosecutions, Keir Starmer QC:

> The guidelines will help prosecutors to make fair and consistent decisions to prosecute in those cases that clearly require robust prosecution in accordance with the Code for Crown Prosecutors . . . .[73]

The guidelines themselves contain information about harassment and stalking, with reference made throughout the document that 'prosecutors should consider the facts of the case carefully, to determine

64. Salter and Bryden (n 20) at 101.
65. Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate (n 12) at 52.
66. SE Ullman, *Sexual Assault: Society's Response to Survivors* (American Psychological Association, USA 2010).
67. DL Payne, KA Lonsway and LF Fitzgerald, 'Rape Myth Acceptance: Exploration of Its Structure and Its Measurement Using the Illinois Rape Myth Acceptance Scale' (1999) 33 Journal Research Personality 27. <https://www.independent.co.uk/news/uk/crime/rape-sexual-history-assault-cross-examine-trial-court-voices4victims-plaid-cymru-mp-liz-savile-a7570286.html> (accessed 3 May 2018).
68. Payne, Lonsway and Fitzgerald (n 67).
69. M Yar, *Cybercrime and Society* (Thousand Oaks, London 2006) 16.
70. *Chambers v DPP* [2012] EWHC 2157 (Admin), [2013] 1 WLR 1833.
71. <http://blog.cps.gov.uk/2012/09/dpp-statement-on-tom-daley-case-and-socialmedia-prosecutions.html> (accessed 2 July 2018).
72. Crown Prosecution Service, *Guidelines on Prosecuting Cases Involving Communications Sent Via Social Media* (HMSO, London 2013).
73. Ibid.

whether the evidence establishes the offences of harassment or stalking'.[74] Yet there continues to be difficulties by both the police and the CPS when it comes to harassment and stalking online.

In June 2017, Molly McLaren ended her seven-month relationship with Joshua Stimpson, after having concerns about his controlling behaviour. Within days Ms McLaren had to approach her local police force after Mr Stimpson started to harass her via the social networking site, Facebook. She made comments to her friends at the time that he had 'lost the plot' and she was in fear of her own life.[75] Despite, her concerns for her own welfare, Mr Stimpson simply received a phone call from officers, warning him about his behaviour. A week after the phone call, Mr Stimpson stabbed Molly 75 times outside a gym in broad daylight, resulting in the force reporting itself to the Independent Office for Police Misconduct.[76]

Sadly, the experiences suffered by Ms McLaren have not been in the minority. Lily Allen, a well-known singer, found herself a victim of online stalking, in 2009. The stalking started with a tweet being sent to her by a stranger. This ended in the perpetrator breaking into her home while she and her children slept. Her stalker had the intention to cause her some form of harm that evening but was fortunately interrupted by a friend of Ms Allen's who was staying with her at the time.[77] Like Ms McLaren, Ms Allen had reported the behaviour to her local police force, however, they were dismissive of her version of events:

> Calling the police back the next day, Allen told them she thought the intruder could be the same man who had been threatening her. 'But they were uncomfortable with the idea. Then I realised my handbag was missing and the change in atmosphere was palpable, it was like a sigh of relief: now it's burglary—we understand that'.[78]

The failures of the criminal justice system to take online conduct more seriously is nothing new. Her Majesty's Inspectorate of Constabulary, in 2015, conducted a report examining the policing of digital crime. Here, they raised concerns that the police were not fully recognising the impact of digital crime on victims:

> We found that some police officers and staff were dismissive of complaints about the misuse of social media sites. We were met with comments such as: '[w]hat do they [the victim] expect us to do about it?' 'I do not use social media; how am I supposed to investigate it?'[79]

Three years later, we are seeing similar attitudes to harassment and stalking conducted online.

In March 2017, Gemma[80] received an anonymous message online, containing explicit material.[81] The message was sent from an account she did not recognise via Facebook. Following the first message being sent, the account was deactivated. However, soon after, new social media profiles emerged continuing the abuse against her: 'The messages included one telling me I should not be afraid of dark alleyways because he preferred the daylight'. As a consequence of the constant abuse, Gemma reported her online experiences to her local police force but was informed, at first, that there was little they could do because of the multiple accounts and because the perpetrator was using a proxy server. Over the course of a few

74. Ibid.
75. <https://www.independent.co.uk/voices/molly-mclaren-stalking-joshua-stimpson-stabbed-theodore-johnson-cps%20a8198836.html?utm_campaign=Echobox&utm_medium=Social&utm_source=Facebook> (accessed 3 April 2018).
76. At the time of writing, the Independent Office for Police Misconduct review into the case of Molly McLaren is still ongoing.
77. <https://www.theguardian.com/music/2016/apr/16/lily-allen-stalked-singer-police> (accessed 3 April 2018).
78. Ibid.
79. Her Majesty's Inspectorate of Constabulary, *Real Lives, Real Crime: A Study of Digital Crime and Policing* (HMIC, London 2015) at para. 6.14.
80. Please note, this is not the victims real name.
81. <http://www.bbc.co.uk/news/uk-england-hereford-worcester-43291038> (accessed 3 April 2018).

months, she continued to receive abusive messages, with little help given to her from the criminal justice system: 'The dismissal by the police made me feel even more isolated'.[82]

The report conducted by the Criminal Justice Inspectorates and HM Crown Prosecution Service Inspectorate in 2017 goes further to find a failure by some police forces to link all conduct undertaken by a defendant together, despite the social media prosecution guidelines empathising the importance of this:

> Where an individual receives unwanted communications from another person via social media in addition to other unwanted behaviour, all the behaviour should be considered together in the round by the prosecutor when determining whether or not a course of conduct is made out.[83]

The guidelines make numerous remarks reminding prosecutors to take into account the PHA, yet there has been a drop-in prosecutions under this Act of Parliament, despite an increase in reports made to police concerning abuse conducted online.[84]

## Protection from Harassment Act: The Future

The criminal justice system, society and social networking sites are struggling to keep pace with the advancements of changing technology. The examples above illustrate a failure by the police and the CPS to link online abusive content to the behaviours of stalking and harassment, resulting in devastating consequences for some individuals. Clearly more needs to be done to protect victims from this form of abuse, from changes in the legal system to better education on the impact of social media. Recently, the government has implemented compulsory education for 5 to 16 year olds in relation to online safety and how to use the Internet respectfully. The purpose of a compulsory national computer curriculum is to ensure:

> all young people are equipped to have healthy and respectful relationships in both the online and offline world, and leave school with the knowledge to prepare them for adult life.[85]

While compulsory education is a positive step forward, further emphasis has been placed on social networking sites to do more to stop online abuse:

> The government cannot keep citizens safe on its own, everyone has a role here: government, industry, parents, civil society and citizens. In particular, we need the technical understanding and expertise of the industry. This is why we will work in partnership with social media and other technology companies, working with them to provide safer online platforms for their users and providing support to do this where it is needed.[86]

Currently, under European Law, social media networks are protected under the e-Commerce Directive (2000/31/EC), as being regarded as hosts rather than publishers, when certain criterions are met. Put simply, social media companies are only under an obligation to remove content from their sites if they have actual knowledge of its existence. Here, in some Members of States, the court will consider how the Internet Society Service provider was made aware of the illegal content and whether the information given to the provider was sufficient to constitute knowledge.[87] If sufficient knowledge is given, service providers must then act 'expeditiously' to remove such content from its site. Despite these obligations, social media companies are slow in their response to the removal of online abuse, as exposed in the work

82. Ibid.
83. Crown Prosecution Service (n 72).
84. <http://www.bbc.co.uk/news/uk-england-41693437> (accessed 30 January 2018).
85. HM Government, *Government Response to the Internet Safety Strategy Green Paper* (HM Government, London 2018) 31.
86. Ibid at 16
87. I Walden in A Büllesbach et al. (eds) *Concise European IT Law* (Kluwer Law International, Netherlands, 2010) 253.

of the Fawcett Society. In August 2017, the Fawcett Society reported several abusive tweets to Twitter, including threats of rape, racist commentary and misogynistic abuse. A week after these comments were reported to Twitter, they were still publicly viewable, this included a video of an apparent rape.[88]

The Home Affairs Committee, in 2017, held a review examining hate crime and extremist content online.[89] Representatives from Facebook, Twitter and YouTube[90] attended the committee meeting to respond to questions posed to them by MPs about their role in containing abusive and extremist content on their sites, where they were heavily criticised:

> The biggest companies have been repeatedly urged by Governments, police forces, community leaders and the public, to clean up their act, and to respond quickly and proactively to identify and remove illegal content. They have repeatedly failed to do so.[91]

Social networking companies are, therefore, not only reluctant in working with the criminal justice system to disclose information contained on their sites but also, they are slow in the application of removing abusive content from their network. The law must, therefore, intervene more adequately to protect individuals from online abuse. Better training of legal personnel within the justice system, clearer legal frameworks and improved education is needed to help tackle this growing problem in society.

In an era where access to social media sites are only a click away, cyber harassment and cyberstalking are becoming more prominent. Victims can be faced with continued contact around the clock and when they turn to the criminal justice system for help are often left frustrated at the lack of support given to them. The Internet, in particular, social media, has become part of many individuals lives, it can no longer be considered as separate from real life.[92] The law and the criminal justice system must, therefore, change its approach in order to help those who become subject to cyber harassment and cyberstalking.

## Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

88. <https://www.fawcettsociety.org.uk/news/twitter-failing-women-experiencing-online-threats-harassment> (accessed 9 October 2018).
89. Home Affairs Committee, *Hate Crime: Abuse, Hate and Extremism Online* (Home Affairs Committee, London, 2016).
90. Only these three Social Networking companies were present as they are the only companies with representatives in the UK.
91. Home Affairs Committee (n 89) at 36.
92. Figures released by the Office of National Statistics found that 90% of men and 88% of women were regular Internet users. <https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2017> (accessed 17 May 2018).