# Rethinking Cyberhate Laws

**Chara Bakalis***

**Contact Details: Chara Bakalis, Principal Lecturer, Oxford Brookes University, cbakalis@brookes.ac.uk**

## ABSTRACT

Cyberhate is a growing problem. There is legislation in place that can be used to tackle various aspects of online hate, but in practice, the existing offences are difficult to use. The law is fragmented, and does not capture the true nature of internet hate or provide adequate protection to victims. This piece evaluates the current provisions and concludes with a framework for creating new legislation to tackle cyberhate which will be easier for the police and prosecutors to use, which will reflect more clearly the harm caused by hate on the internet, and which is also compatible with freedom of expression.

## KEY WORDS

Cyberhate – online abuse – hate speech – hate crime

Cyberhate is a growing problem. Although we do not have official statistics that can give as an accurate picture of the actual amount of online hate, several recent studies have found alarming levels of abuse. For example, Tell MaMa reports that 70% of instances of Islamophobic hate reported to them is online hate,[1] whilst the CST has found that over 20% of anti-semitic hate they record is internet-based.[2] A survey by Galop suggests that 84% of LGBT+ people have experienced at least one occurrence of online abuse,[3] whilst Ofcom reports that a third of children between the ages of 12-15 have been exposed to online hate speech.[4] This is backed up

---

* Principal Lecturer in Law, Oxford Brookes University

1 The figures have varied from year-to-year, but in 2014-15, online hate made up 70% of the reported incidents of Islamophobic hate - https://www.tellmamauk.org/wp-content/uploads/pdf/Tell%20MAMA%20Reporting%202014-2015.pdf accessed on 29 September 2017

2 See page 27 at https://cst.org.uk/data/file/d/f/CST_Annual_Review_2016.1486995234.pdf - accessed on 29 September 2017

3 http://www.galop.org.uk/wp-content/uploads/2017/08/Online-hate-report.pdf accessed on 29 September 2017

4 https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf accessed on 29 September 2017

by statistics from the NSPCC which suggest that 1 in 4 children has come across a racist or hate message online.[5] An analysis by the think-tank Demos found that in the week following the Brexit referendum in June 2016, over 13,000 xenophobic or anti-immigrant tweets were sent on Twitter,[6] and the UK Safer Internet Centre published a report that found that one in 4 children have suffered abuse online because of disability, race, sexual orientation, transgender identity or religion.[7]

There is legislation in place that can be used to tackle various aspects of cyberhate, but in practice, the existing offences are difficult to use. The law is fragmented, and there are several pieces of legislation at the disposal of the police and CPS depending on how the cyberhate manifests itself.[8] The existing offences also do not capture the true nature of internet hate as the offences were either created before the dawn of the internet, or are not aimed at protecting victims of cyberhate. As a result, one estimate suggests that only 9% of online hate is investigated.[9]

This article will adopt a broad definition of cyberhate that encompasses any use of technology to express hatred[10] towards a person or persons because of a protected characteristic – namely race, religion, gender, sexual orientation, disability and transgender identity.[11] This definition will capture a great deal of activity that currently takes place on the internet, or through email and mobile telephone technology such as: religious abuse aimed at individuals by SMS text messages, anti-disablist comments aimed at a specific person on Twitter, racist statements appearing in below the line comments on newspaper websites, blogs devoted to homophobic and transgender hate, and misogynistic conversations on discussion forums.

This article will evaluate the four main pieces of legislation currently used by the police and the CPS to tackle online hate crime in England and Wales, and will consider to what extent the law is

---

5 https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/facts-statistics/ accessed on 29 September 2017

6 https://www.demos.co.uk/project/hate-speech-after-brexit/ accessed on 29 September 2017

7 https://www.theguardian.com/uk-news/2016/feb/09/internet-trolling-teenagers-online-abuse-hate-cyberbullying accessed on 29 September 2017

8 See for example the Digital Trust's Criminal Offences (Misuse of Digital Technologies and Services) Bill which aims to consolidate the disparate law in this area - http://www.digital-trust.org/victims-bill/technologybill accessed on 29 September 2017

9 https://hansard.parliament.uk/Commons/2016-07-07/debates/16070729000001/OnlineAbuse accessed on 29 September 2017

10 There is a rich body of literature within hate crime academics discussing which is the most appropriate word to refer to this type of legislation. See Nathan Hall *Hate Crime* (Routledge, 2nd edn, 2013) Chapter One. The legislation in England and Wales has adopted the use of 'hostility' and 'hatred'. For the purposes of this article, a broad definition will be adopted.

11 With the exception of gender, these characteristics are the ones currently covered by s.145 and s.146 of the Criminal Justice Act 2003. It will be explained below why gender should be added to the list.

able to deal satisfactorily with cyberhate in cases where the individual perpetrator can be identified and brought to justice.[12] It will be argued that whilst the law is able to cover some aspects of cyberhate, it is not able to deal with the full spectrum of internet hate. This is because the current legislation does not make a sufficient distinction between the different ways in which cyberhate can cause harm to individuals and society. Thus, whilst the CPS has recently stated that it is determined to crack down on social media hate,[13] the existing legal provisions are inadequate, and there is an urgent need for reform. The piece will conclude with a framework for creating new legislation to tackle cyberhate which will be easier for the police and prosecutors to use, which will reflect more clearly the harm caused by hate on the internet, and which is also compatible with freedom of expression.

## Current Legislation

There are several pieces of legislation that could potentially be used by prosecutors in cases involving cyberhate.[14] In fact, the large number of available offences is one of the reasons why law enforcers have found this a difficult area to prosecute.[15] However, four pieces of legislation appear to be the main focus of the literature: the Public Order Act 1986, the Protection from Harassment Act 1997, the Malicious Communications Act 1988, and the Communications Act 2003. The offences under these acts can be divided into two categories. The first category includes offences which apply both to online and offline communications, and which have been specifically designed to deal with hatred or hostility. The second category of offences are those which have been created to apply to online offences, but which are not specifically designed to deal with online behaviour that is hateful or hostile. The existing offences will be analysed and their main flaws and problems will be highlighted.

---

12 It will not deal with cases where perpetrators remain anonymous because this category of cyberhate needs separate consideration as it involves a discussion of the role of third party intermediaries. This has recently been discussed by the Report of the Home Affairs Committee Report on Hate Crime and its Violent Consequences Inquiry, 'Hate Crime: abuse, hate and extremism online' https://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/60902.htm accessed on 29 September 2017. Cases such as *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014) and *Delfi AS v. Estonia* 64669/09 (2015) will not be discussed.

13 https://www.theguardian.com/society/2017/aug/21/cps-to-crack-down-on-social-media-hate-says-alison-saunders accessed on 29 September 2017

14 See for example the Digital Trust's Criminal Offences (Misuse of Digital Technologies and Services) Bill which outlines the many pieces of legislation which can be used in this area - http://www.digital-trust.org/victims-bill/technologybill accessed on 29 September 2017

15 https://www.theguardian.com/uk-news/2016/mar/04/online-abuse-existing-laws-too-fragmented-and-dont-serve-victims-says-police-chief accessed on 29 September 2017

## A) Offences designed to deal with hatred or hostility

First to be considered are three sets of offences: firstly, the offences of 'harassment'[16] and 'stalking'[17] under the Protection from Harassment Act 1997 (hereafter "PHA"); secondly the 'public disorder' offences under sections 4, 4A and 5 of the Public Order Act 1986 (hereafter "POA"); and thirdly, the 'incitement to hatred' provisions under Part III of the POA;

These offences can all be loosely described as 'hate crimes'. The term 'hate crime' does not have a specific legal meaning, but has been used flexibly to describe any legislation or legal response aimed at punishing criminal behaviour which demonstrates either hatred, or hostility[18] towards a particular group in society.

The public disorder offences and the harassment and stalking offences can all become 'aggravated offences' by virtue of sections 31-32 of the Crime and Disorder Act 1998 (hereafter "CDA"). The CDA makes a crime an aggravated offence when a defendant demonstrated or was motivated by hostility towards a person on the grounds of race and religion[19] in the course of committing a 'basic offence'. The list of basic offences is a closed one but does include the public disorder and harassment and stalking offences to be discussed here. The aggravated version of an offence attracts a higher maximum penalty than the basic offence. For example, the maximum penalty for a s.4 POA offence increases from 6 months to two years when aggravated by racial or religious hatred.[20]

The 'incitement to hatred' offences were enacted to deal with hateful behaviour. These offences have a long history[21] rooted in anti-discrimination legislation, but in their current form they seek to criminalise behaviour which is threatening, abusive or insulting where there is an intention to thereby stir up racial hatred, or, having regard to all the circumstances, racial hatred was likely to

---

16 Protection from Harassment Act 1998, ss2 and 4. Section 4 covers the offence of putting someone in fear of violence.
17 Protection from Harassment Act 1998, ss2A and 4A.
18 Or bias or discrimination
19 Aggravated offences in relation to racial hostility were enacted under the Crime and Disorder Act 1998, ss28-32, and racially aggravated offences were added by the Anti-terrorism, Crime and Security Act 2001, s 39.
20 Crime and Disorder Act 1998, s 31(4)(b).
21 See for instance, Gavin Schaffer, 'Legislating against Hatred: Meaning and Motive in Section Six of the Race Relations Act of 1965' (2014) 25 *Twentieth Century British History,* and Ivan Hare, 'Legislating Against Hate – The Legal Response to Bias Crimes' (1997) 17 OJLS 415.

be stirred up thereby. These offences have now been extended, albeit in a more limited way, to religious and sexual orientation hatred.[22]

In evaluating the effectiveness of the provisions under the POA and the PHA to enable the police to prosecute cyberhate, it is important to note at the outset that these offences are of general application and are not specifically targeted at online communications. This means that it can be difficult to properly assess their efficacy as the Ministry of Justice data for these offences does not currently disaggregate online and offline use of these provisions.[23] However, the assessment of the reported case law in this area which follows indicates that the courts have faced some technical difficulties in applying offline offences to online behaviour, and this has limited the effectiveness of these provisions. Furthermore, it will be argued that these offences are not able to adequately capture the harm caused to victims of cyberhate and so there is a need to create separate offences targeted at the online communication of hate.

### 1) Protection from Harassment Act 1997 ("PHA")

The PHA makes it an offence to carry out a course of conduct which amounts to harassment[24] and stalking.[25] [26] The mens rea is to know or ought to know that the behaviour amounts to harassment or stalking.[27] As outlined above, if the defendant is motivated by or demonstrated hate whilst committing one of these offences, then this becomes an aggravated offence which increases the maximum penalty.[28] The offences are result crimes which means that a victim must be identified, and to be shown to have suffered tangible harm. There is no definition of 'harassment' but it is defined to 'include'[29] causing someone alarm or distress. The Supreme Court in *Hayes v Willoughby*[30] defined harassment as a 'deliberate course of unreasonable and oppressive conduct, targeted at another person, which is calculated to and *does cause* that person alarm, fear or distress' hence confirming that this is a result crime. The harm which

---

22 The offences were extended to 'religion' by the Racial and Religious Hatred Act 2006, and to 'sexual orientation' by the Criminal Justice and Immigration Act 2008
23 See, for example, the Ministry of Justice's most recent figures: https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2015 accessed on 29 September 2017. Use the 'Outcome by Offence' table.
24 Protection from Harassment Act 1997, ss 2 and 4
25 Protection from Harassment Act 1997, ss 2A and 4A
26 Protection from Harassment Act 1997, s 3 also makes harassment a civil wrong.
27 Protection from Harassment Act 1997, s 1(1)(b)
28 Crime and Disorder Act 1998, s 32
29 Protection from Harassment Act 1997, s 7
30 *Hayes v Willoughby* [2013] UKSC 17

needs to be proven under sections 4 and 4A is to fear that violence will be used against them or the victim is caused serious alarm which disrupts their day-to-day life.

Whilst these offences were not created specifically with the internet in mind, they can go some way towards protecting individual victims who have been targeted online by a perpetrator. In 2009, Kelly Houghton became the first person to be jailed for harassment for sending threatening messages via Facebook. Since then, the courts have continued to use the PHA to prosecute cases of cyber-harassment. The recent case of *R v Cordle*[31] is a good example of how the offence is used. In this case, the defendant had sent text messages to his victims, as well as emails and messages on social media, all of which, in conjunction with offline behaviour, combined to form a course of conduct falling within the PHA. Whilst currently there are no reported cases of racially or religiously aggravated harassment where technology was used, there have been successful prosecutions of offline aggravated harassment.[32]

These cases demonstrate that the PHA can be used in some instances to protect victims of cyberhate harassment. It is, however, difficult to find evidence to help us evaluate how effective this legislation is in practice. The CPS and Ministry of Justice publish separately figures on the number of successful harassment prosecutions[33] and on the CDA aggravated versions of these offences.[34] However, the figures on harassment refer specifically to harassment against women and girls, and they do not tell us whether these were for online or offline behaviour. The figures also do not disaggregate offences by how they were committed, so these figures cannot tell us how frequently these provisions are used against online behaviour; nor do they tell us how frequently the s.32 racial and religious aggravation offences are prosecuted. The Hate Crime Report and the accompanying data also do not cover this as there is no disaggregation by offence or by mode of commission of offence.[35] There is, therefore, an obvious problem in assessing the success of a provision in combatting cyberhate when the offence can be used for both online and offline behaviour. A separate offence targeted specifically at online behaviour would make it easier to monitor and evaluate its efficacy as data which focusses exclusively on online hate could be more easily produced and analysed. We do know, however, that the police have felt

---

31 *R v Cordle* [2016] EWCA Crim 1793
32 For example, *Jones v DPP* [2010] EWHC 523 (Admin)
33 See for example the Violence Against Women and Girls report 2015-16 http://www.cps.gov.uk/publications/docs/cps_vawg_report_2016.pdf accessed 29 September 2017
34 See for example Hate Crime report 2014-15 and 2015-16 https://www.cps.gov.uk/publications/docs/cps_hate_crime_report_2016.pdf -accessed on 29 September 2017
35 In fact, the PHA does not even appear as one of the 'principal offences' by strand - Hate Crime report 2014-15 and 2015-16 https://www.cps.gov.uk/publications/docs/cps_hate_crime_report_2016.pdf -accessed on 29 September 2017 page 32

overwhelmed by the amount of hate and are finding the law difficult to use[36] and the CPS has sought help from Twitter in order to cope with the increasing amount of online abuse.[37]

There does, appear, however to be some evidence that the PHA is not necessarily the preferred legislation in online communications. Geach and Haralambous[38] have pointed out an interesting interplay between the Malicious Communications Act 1988 (discussed in more detail below) and the PHA. In 2001, the Malicious Communications Act was updated to include online communications. Once that change was implemented, Geach and Haralambous state that the CPS began to utilise this offence more than the PHA, even for cases involving online harassment.[39] Furthermore, Coe offers evidence that suggests s.127(1)(a) of the Communications Act 2003 (also discussed in more detail below) is increasingly becoming the preferred option, even for online bullying cases with a seven-fold increase in the use of this offence from 2011/12 to 2013/14.[40]

Looking beyond issues relating to collecting data on the use of these offences, there are some obvious constraints within the framework of the PHA that would explain why it has not been used as extensively as it could be for online behaviour. As Salter and Bryden have pointed out, the requirement for a 'course of conduct'[41] under the PHA is a potential problem for online communications as it means that one-off communications will not count.[42] Thus, an individual sending a racially abusive email to thousands of people would not be covered by the PHA.[43] Another limitation of the PHA is how it responds to covert surveillance over the internet. A disagreement has arisen in the literature about the ambit of the stalking offences.[44] McEwan argues that covert surveillance of a victim via the internet will not be covered by these offences because, by definition, covert surveillance is unknown to the victim. This means that the victim

---

36 http://www.telegraph.co.uk/news/uknews/crime/11653092/Police-facing-rising-tide-of-social-media-crimes.html accessed on 29 September 2017

37 https://www.theguardian.com/technology/2016/mar/03/twitter-to-train-prosecutors-in-fight-against-online-abuse accessed on 29 September 2017

38 Neal Geach and Nicola Haralambous, 'Regulating harassment: is the law fit for the social networking age?' (2009) 73(3) Jounrnal of Criminal Law 241

39 Neal Geach and Nicola Haralambous, 'Regulating harassment: is the law fit for the social networking age?' (2009) 73(3) Jounrnal of Criminal Law 241

40 Peter Coe, 'The social media paradox: an intersection with freedom of expression and the criminal law' (2015) 24 Information & Communications Technology Law 16, 39-40

41 Protection from Harassment Act 1997, s 1(1)

42 Micheal Salter and Chris Bryden, 'I *can* see you: harassment and stalking on the Internet' (2009) 18(2) Information & Communication Technology Law 99

43 Example from Micheal Salter and Chris Bryden, 'I *can* see you: harassment and stalking on the Internet' (2009) 18(2) Information & Communication Technology Law 99, 122

44 Neil MacEwan, 'The new stalking offences in English law: will they provide effective protection from cyberstalking?' (2012) 10 Criminal Law Review 767; Alisdair A. Gillespie, 'Cyberstalking and the law: a response to Neil MacEwan' (2013) 1 Criminal Law Review 38;

will not have experienced the requisite fear, alarm or distress, or fear of violence required by these offences.[45] By contrast, Gillespie argues that where covert surveillance is discovered and thus, becomes known to the victim, this will be covered by the PHA if the victim suffers the harm required by the Act.[46] Furthermore, he argues that even if the PHA cannot itself deal with the covert targeting of a victim's computer technology, alternative provisions under the Computer Misuse Act 1990 and the Regulation of Investigatory Powers Act 2000 can be used instead.

Even if we are to accept Gillespie's view, this disagreement about the scope of the legislation, is a good example of the fragmented nature of the current law in relation to online harassment. It demonstrates the difficulties the prosecution face when dealing with online harassment where several pieces of legislation could potentially be used depending on the fine nuances of the facts. When one considers this in the context of cyberhate, this problem is compounded further. This is because whilst the PHA is an aggravated offence under the CDA, the Malicious Communications Act 1988, the Computer Misuse Act 1990 and the Regulation of Investigatory Powers Act 2000 are not. This means that certain forms of behaviour carry the additional penalty of an aggravated offence, whilst other forms of behaviour will not. For example, if a perpetrator, motivated by racial hostility, were to hack into a victim's computer and send messages from the victim's email account, this would be an offence under the Computer Misuse Act and the Regulation of Investigatory Powers Act, and the racial hostility would be taken into account at the sentencing stage of the offence only.[47] However, if the victim were to become aware of the fact that their account had been hacked into and this caused them to suffer alarm, fear or distress, this would come under the PHA and the racial hostility would be taken into account at the offence stage, and would result in a higher maximum penalty. This serves to illustrate the confusion that must arise at the prosecutorial stage when deciding which piece of legislation to charge.

Another problem with the PHA is that it cannot be used for prosecuting comments not directed at the victim themselves, such as, for example, where someone has posted several aggressive and threatening anti-Islamophobic tweets on Twitter which are not directed at anyone in particular. It is doubtful that these posts would be considered harassment as the Supreme Court has

---

45 Neil MacEwan, 'The new stalking offences in English law: will they provide effective protection from cyberstalking?' (2012) 10 Criminal Law Review 767

46 Alisdair A. Gillespie, 'Cyberstalking and the law: a response to Neil MacEwan' (2013) 1 Criminal Law Review 38

47 Criminal Justice Act 2003, ss. 145-146

recently stated in *Hayes v Willoughby*[48] that harassment is the 'conduct targeted at another person'.[49]

This limitation of the harassment and stalking offences in relation to online hate demonstrates that the mischief at the heart of the PHA may not necessarily be ideally suited to the harm caused by online hate. The PHA is concerned with the relationship between the harasser and the person who is being harassed. It was designed to deal with situations where a person fears for their physical integrity because of the pattern of behaviour by the harasser. The PHA is limited to the harasser/harassee relationship and does not extend to a bystander who may have observed the interchange between the two, or to cases where the hateful comments are not directed at anyone in particular. Given that the internet, and particularly social media, gives people access to a very large audience, many instances of cyberhate will simply not fall into the purview of the PHA.

This leads to an important question at the heart of the debate about the regulation of cyberhate, which is whether the regulation of cyberhate requires us simply to ensure that existing offences dealing with offline behaviour are modified so that they also apply online; or whether the harm caused to victims of cyberhate and to society more generally is sufficiently different to necessitate separate regulation in the form of discrete online hate offences. In the context of cyberstalking, McEwan has argued that the offence is different in nature to ordinary stalking because it widens the pool of potential victims, it creates new ways in which a victim can be stalked, the stalking can be more intense because perpetrators feel less inhibited than in real life, and the anonymity of the internet often means that the stalking is more vitriolic.[50]

A major theme of this paper will be to answer this central question and will be discussed in more detail below. However, at this point it seems clear that the PHA will only offer protection to victims of cyberhate in cases where the perpetrator can be identified, where they have targeted their hate at one person or persons directly on more than one occasion, and where the targeted victim/s themselves have suffered harassment, alarm or distress.

---

[48] *Hayes v Willoughby* [2013] UKSC 17

[49] Although in *R (A Child) v DPP* [2001] EWHC Admin 17 the Divisional Court held that behaviour not directed at the victim could come within the PHA, on the facts of the case, the court was persuaded by the fact that the victim was 'in the presence' of the defendant when he was making threats to the victim's dog. Even if it could be said that Twitter users are 'in the presence of threats' made on Twitter, it was later clarified in the case of *R v Qosja (Robert)* [2016] EWCA Crim 1543 that the victim needs to fear that violence *will* be used against them, and not merely that it *might*. It is difficult to see how general hateful messages on Twitter could satisfy this requirement.

[50] Neil MacEwan, 'The new stalking offences in English law: will they provide effective protection from cyberstalking?' (2012) 10 Criminal Law Review 767

## 2) Public Disorder Offences

The next set of offences to consider are the public disorder offences under s.4, s.4A and s.5 of the POA. Under s.4 of the POA it is an offence to use towards another person any words or behaviour or to display any writing or sign or other visible representation which is threatening, abusive or insulting. The mens rea for this offence is an intent to cause that person to believe (or likely to believe) that unlawful violence will be used against them or another, or to provoke such violence by that person or another. Under s.4A of the Act, an offence is committed if a person uses words, behaviour, writing, sign or other visible representation which is threatening, abusive or insulting, and which causes that or another person harassment, alarm or distress, and with intent to do so. And finally, s.5 makes it an offence to use words, behaviour, writing, sign or other visible representation which is threatening or abusive within the hearing or sight of a person likely to be caused harassment, alarm or distress. There are racially and religiously aggravated versions of these offences under the CDA.[51]

In order to evaluate to what extent these offences are able effectively to tackle online communications, the important case of *S v DPP*[52] needs to be considered. In this case, the defendant, who was protesting against animal testing at a lab, uploaded a picture of the victim - a security guard at the lab - onto a publicly available website, and implied, falsely, that the victim had convictions for violent offences and had manhandled protestors. The police saw the photos, downloaded them, and about five months after they were first uploaded to the internet, they showed the victim copies of the photos. Up until this point, although the victim was aware of the presence of the photos online, he had not actually viewed them on the relevant website. Crucially, it was not clear on the facts whether the photos were still available online at the point at which the victim was shown the copies. The defendant was nevertheless convicted of a s.4A offence on the basis that the victim was caused harassment, alarm, or distress on being shown copies of the photos by the police, coupled with the knowledge that these photos had at some time been available on the internet. The defendant subsequently appealed arguing that a substantial period of time had passed since the uploading of the photo, and so there was no sufficient nexus or causal link between the uploading and the subsequent harassment, alarm, or distress experienced by the victim, particularly given that there was no evidence that the material

---

51 Crime and Disorder Act 1998, s 31

52 *S v DPP* [2008] EWHC 438 (Admin)

was still available online at that moment. His appeal was dismissed. The court found it to be irrelevant whether or not the photos were still on the internet, and they said that the test to apply was: but for the defendant's actions, the victim would not have suffered, harassment, alarm or distress; they also concluded that the passage of time did not break the chain of causation.[53]

Although this is an example of a case where there was a successful prosecution against a person who had uploaded material on the internet, it is clear that s.4A was never intended to deal with instant and asynchronous messages, and so the judges in this case were put under pressure to interpret the statute in such a way as to fit the facts.[54] This resulted in a number of doctrinal issues being overlooked, distorted or confused.

Firstly, there is the finding that the defendant does not need to be present at the time that the victim views the offending material. This goes against previous case law which suggests that the defendant must be present at the time that the harassment, alarm or distress is caused. For example, *Chappell*[55], confirmed the requirement that the defendant be present at the time of the offence. In this case a defendant was found not guilty of a s.5 offence where a woman had opened a threatening letter without the defendant there. The court in *S v DPP* distinguished this case on the basis that the wording of s.5 states that the behaviour complained of must be 'within the hearing or sight of a person likely to be caused harassment, alarm or distress thereby', whereas this wording does not appear in s.4A or s.4. This would, therefore, rule out s.5 as being able to be used in the vast majority of cyberhate cases but would allow s.4A and s.4 to be used. The judges speculated that this omission was potentially purposeful as s.4A was enacted in 1994 and so was created with the internet in mind. However, as the judges themselves point out, s.4A - as does s.4 - gives a defence to the perpetrator if they were 'inside a dwelling' at the time of committing the relevant act and the victim was also in that or another 'dwelling'. This defence makes it highly unlikely that the offence was created with the internet in mind given that it would give a defence to anyone who uploaded material whilst in a dwelling, and the material was viewed whilst in a dwelling. This fact was acknowledged by the judges in *S v DPP*[56], but it was not acknowledged that this severely undermines the argument that the omission of 'within the hearing or sight' of the victim in s.4A was intentional in order to cover cases on the internet.

---

53 As an aside, the court did not explicitly mention legal causation but this can be implied from their application of *novus actus interveniens*

54 Chris Newman, 'Offensive picture on the internet later shown to complainant by a third party causing distress' (2008) 72(6) Journal of Criminal Law 481

55 *Chappell v DPP* [1989] 89 Crim App R 82

56 *S v DPP* [2008] EWHC 438 (Admin), para. 12

A second problematic aspect of the case was how the public order element of the offence was dealt with. Central to these offences is the need for the behaviour to be carried out in the public domain. This is made clear by the inclusion of the dwelling defence, and cases such as *Holloway v DPP*[57] which state that it is not the intrinsic nature of the behaviour that makes it criminal, but the fact that it is carried out in 'public'. Without this, these offences cease to be public order offences and become offences against the person. The court in *S v DPP did* recognise the public order nature of s.4A by accepting without question the district judge's decision that uploading material to the internet automatically puts it into the public domain. However, somewhat confusingly, the court also went on to find that it was irrelevant whether the material was still present on the internet at the time the victim was caused harassment, alarm, or distress.[58] The court relied on the unreported case of *Rogers v DPP*[59] where it was decided that the victim had been caused harassment, alarm or distress when watching violent demonstrations via CCTV. However, in *Rogers*, the victim was watching the demonstration simultaneously with the event unfolding in real life, and not after the event had occurred. This would suggest that to satisfy the public order element of this offence, and to be consistent with *Rogers*, the material would have to have been shown to be present on the internet at the time of the offence. Without this, it is difficult to see how the public order element in *S v DPP* was fully satisfied.[60]

A final point to make here is that, in addition to the doctrinal issues outlined above, s.4A, like the PHA offences, is a result crime as it requires the victim to have been caused harassment, alarm, or distress. This means the offence can only be committed when a tangible harm to the victim has occurred. This raises the question about what should the mischief be at the heart of cyberhate offences: should the focus be on the harm caused by the perpetrator to the victim, or should the focus instead be on the conduct of the defendant? This issue strikes at the heart of the underlying rationale for these offences and requires deep consideration of the harm caused by online hate. This will be considered in more detail below.

This analysis of *S v DPP* suggests that whilst s.4A and s.4 can potentially be used against a perpetrator of cyberhate, they are of limited use. This is not surprising given that they were not created with the intention of covering internet-based offence. Whilst the judges in *S. v DPP* did

---

57 *Holloway v DPP* [2004] EWHC 2621 (Admin)

58 Coe makes a similar point in Peter Coe, 'The social media paradox: an intersection with freedom of expression and the criminal law' (2015) 24 Information & Communications Technology Law 16, 39-40

59 *Rogers v DPP* (unreported) 22 July 1999, CO/4041/98

60 It should be noted that in the case of *R v Liam Stacey* who was convicted of the s. 4A offence for tweeting racist comments on Twitter about the footballer Fabrice Muaba, the comments were available online and were viewed online https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/Judgments/appeal-judgment-r-v-stacey.pdf accessed on 29 September 2017

make an attempt to expand s.4A to fit the facts of this particular case, inevitably there are limits to how far this can extend.

### 3) Incitement to Hatred Offences

Part III of the POA creates several offences relating to the incitement of racial, religious and sexual orientation hatred. Under s.18-22 of the POA it is an offence to use words or behaviour or display written material, publish or distribute written material, make public performance of a play, distribute, show or play a recording, broadcast or include in a cabling programme anything which is threatening, abusive or insulting either with an intention to stir up hatred, or where racial hatred was likely to be stirred up thereby. These offences were extended to religious and to sexual orientation hatred,[61] albeit with some material differences that make it harder for the prosecution to prove that the offence has been made out.[62]

Although these provisions were not enacted with the internet in mind, in *Sheppard and Whittle,*[63] Part III of the Act has been interpreted to include material written on the internet.[64] In this case, Whittle emailed Sheppard some Holocaust-denial material. Sheppard edited the material and then uploaded it to a website which he had set up himself, but which was hosted by a remote server in California. The material posted on the website was accessible within the jurisdiction of England and Wales. Sheppard and Whittle were convicted of several counts of s.19 of the POA, but appealed on the basis that the material was published in the US where such content would not be criminalised. The court, however, confirmed the substantive (as opposed to the formal) test of jurisdiction[65] laid down in *Wallace Duncan Smith (No. 4*) which determines jurisdictional issues based on whether a substantial measure of the activities which make up the crime took place in this country. The court determined that because the defendants were based in this country and the material was written, edited, and uploaded in this country, and that the defendants had control of the website which was clearly aimed at people in this country, there was no question that the court had jurisdiction over their material. Thus, the court was not

---

61 The offences were extended to 'religion' by the Racial and Religious Hatred Act 2006, and to 'sexual orientation' by the Criminal Justice and Immigration Act 2008.

62 For example, the provisions relating to religion and sexual orientation have a narrower men rea which is limited to an intention to stir up hatred. Furthermore, for religion and sexual orientation, only threatening words are sufficient. Finally, under s. 29 J of the act there is a freedom of expression provision that expressly defends people's right to, amongst other things, criticise or abuse religion or discuss or criticise sexual conduct or practices.

63 *Sheppard and Whittle* [2010] EWCA Crim 824

64 Matthew Dyson, '*R. v Sheppard (Simon Guy)*: Public order on the internet' (2010) 2 Archbold Review 6-9

65 Matthew Dyson, '*R. v Sheppard (Simon Guy)*: Public order on the internet' (2010) 2 Archbold Review 6-9

convinced by the defendants' arguments that because the server was based in the US, the material was also published in the US, and therefore subject to US criminal law.

Whilst in this case the defendants were found guilty of the relevant offences, there are several problems with the reasoning of the *Sheppard* case that means the scope of the provisions and how they relate to the internet are still unclear.

For example, in terms of jurisdiction, on the facts of the case, it did make sense to confirm *Wallace Duncan Smith (No. 4)*: it was clear in this case that most of the crime had taken place in England and Wales as the defendants were located here, they wrote and edited the material here, and the material was directed at an audience in this country. However, it is unclear what would be the outcome of such a case if the facts differed. For instance, would the courts have found jurisdiction if Sheppard and Whittle had used a server in the US, the material was clearly aimed at an audience in this country, but the defendants were based in France? Or what if Sheppard and Whittle and the server they used had been based in England, but the material was directed at a German audience? It is not clear from the reasoning in *Sheppard* what would have been the outcome. And yet these are scenarios that are very likely to arise. The Court of Appeal did mention three different jurisprudential theories in relation to publications on the internet. The first is that jurisdiction lies with the country in which the server is hosted (the country of origin theory). The second is the country of destination theory which says that jurisdiction lies with the country in which the material is downloadable and the third theory is that jurisdiction lies with the country that was targeted by the defendants – the directing and targeting view.[66] It would have been interesting to discover the view of the court on this, but they declined to comment given that they had already confirmed the *Wallace* case, and had rejected the country of origin theory as the facts did not require them to express a preference. However, this does mean we cannot be certain what would happen in other scenarios, such as those outlined above. The French case of *Yahoo*[67] does appear to have opted for a broader interpretation of jurisdiction to take the country of destination view to say that jurisdiction exists wherever the material is downloadable.[68] However, *Sheppard* did not appear to go this far.

---

66 Uta Kohl, *Jurisdiction and the Internet* (Cambridge: CUP, 2007) at pp 24-32.

67 *LICRA et UEJF v Yahoo! Inc. and Yahoo! France* – Tribunal de Grande Instance de Paris (Superior Court of Paris)

68 Matthew Dyson, '*R. v Sheppard (Simon Guy)*: Public order on the internet' (2010) 2 Archbold Review 6

Another issue with *Sheppard* lies in the definition of 'publication' adopted in this case. The court opted to confirm the definition set out in *Perrin*[69] which defined a publication under the Obscene Publications Act 1959 as 'making available … material to any viewer who may choose to access it'. As Dyson has pointed out, on the facts of this case there is no evidence that anyone other than the police officer downloaded the material.[70] This broad definition of publication is also problematic when applied to the internet as it means that everything uploaded to the internet is 'published' and therefore subject to the same rules and regulations. However, this approach may not be appropriate for the internet where a more nuanced approach may be needed. Account should be taken of the different ways in which material is presented on the internet, and how easily accessible it is. Whilst all material is accessible in theory, anything which appears in, for example social media or below the line comments of newspapers, is likely to have a much wider audience than a stand-alone website, and so this needs to be taken into account when prosecuting such behaviour.

Finally, it needs to be pointed out that whilst prosecutions under Part III are obviously possible, at least to an extent as evinced by *Sheppard*, the high threshold of these offences in other regards means that there are very few successful prosecutions in any given year, particularly in relation to religion and sexual orientation.[71] This is because the wording of the offences is very tight due to fears that doing otherwise would give the police and CPS too much power to prosecute legitimate free speech.[72] According to a recent study by Iganski et al, it seems that these fears are misplaced and it is argued that the CPS has been exercising its power legitimately and has remained within the boundaries of free speech.[73] However, it could be argued given the tiny amount of successful prosecutions for this offence – both offline and online – it would be appropriate to consider whether the threshold is too high.[74]

---

69 R *v Perrin* [2002] EWCA Crim 747
70 Matthew Dyson, 'R. *v Sheppard (Simon Guy)*: Public order on the internet' (2010) 2 Archbold Review 6
71 For example, there was only one prosecution for stirring up hatred in 2014/2015, and one in 2015/16. See https://www.cps.gov.uk/publications/docs/cps_hate_crime_report_2016.pdf accessed on 29 September 2017
72 See for example Ivan Hare 'Crosses, crescents and sacred cows: criminalising incitement to religious hatred' (2006) Public Law 521 for some of the arguments against such provisions.
73 Paul Iganski, Abe Sweiry and Jonathan Culpeper, 'A question of faith? Prosecuting religiously aggravated offences in England and Wales' (2016) 5 Criminal Law Review 334
74 In fact, the small number of prosecution led the Law commission to decide not to extend to other characteristics because there was little evidence that the kind of speech that would be captured by the act exists. This is slightly tautologous as the issue may be to do with the threshold being too high – see Chara Bakalis 'Legislating Against Hatred: The Law Commission's Report on Hate Crime' (2015) 3 *Criminal Law Review* 177 on this point.

In conclusion, it can be see that the current hate crime offences – the PHA, and both sets of POA offences – can provide some help to some cyberhate victims, but they are limited in their ambit as they were not created for online communications. The next section will assess to what extent the offences which were designed with the internet in mind are better able to protect victims of cyberhate.

### B) Statutes designed to apply to the internet

Two offences will be considered in this section – s.1 of the Malicious Communications Act 1988 and s.127(1) of the Communications Act 2003. Both these provisions have been designed to deal with online behaviour, but, unlike the offences discussed above, they have not been specifically created to deal with hate and hostility and they cannot be aggravated under the CDA; although, as is the case with virtually all other crimes, any demonstration or motivation of hostility against race, religion, sexual orientation, transgender identity or disability must be taken into account at the sentencing stage.[75] If the MCA or the CA offences are used in a case of cyberhate, the victim in that instance will receive less protection for the hostility element of the offence than a victim of a public disorder offence or harassment or stalking offences because unlike those provisions, the hate or hostility does not form a constituent part of the offence and so does not appear on the perpetrator's record, and neither can it increase the maximum penalty.[76]

#### 1) S.1 Malicious Communications Act 1988 (hereafter "MCA")

S.1 of the MCA[77] makes it an offence to send to another person an electronic communication which is in whole or part indecent or grossly offensive. The mens rea of the offence is to send the message with the purpose of causing distress or anxiety to the recipient, or to any other person to whom he intends that it or its contents or nature should be communicated.

At the outset, it is important to note that the core of this offence lies in the sending of a communication which is indecent or grossly offensive, with the requisite mens rea.[78] This means that the impact on the victim is not important. In fact, even if the intended victim does not

---

75 Criminal Justice Act 2003, ss. 145-146

76 This is further complicated by the fact that the CDA offences only apply to race or religion, whilst s. 145 and s. 146 apply to race, religion, sexual orientation, transgender and disability.

77 Section 1 as amended by Criminal Justice and Police Act 2001, s 43

78 As confirmed in Supreme Court case of *DPP v Collins* [2006] UKHL 40

receive the message at all, or if the victim does receive the message but is not in fact caused distress or anxiety, the offence is still made out. It is, therefore, a conduct crime. This is in sharp contrast to the PHA offences and s.4A of the POA discussed above which require it to be shown that the victim was caused harm. As mentioned above, this raises an important question about the appropriate regulation of cyberhate: should we punish the conduct of the perpetrator or the effect of their behaviour? This point will be developed further below.

The MCA has been used extensively in relation to online communications on social media, but also in cases involving harassment. The latest figures from the Ministry of Justice show that the number of prosecutions under the MCA has gone up dramatically with 122 prosecutions in 2005 rising to a high of 897 in 2014, although we cannot know how many of these involved cyberhate.[79] There is some evidence that the CPS has preferred to use the MCA and the CA even in cases of harassment as these offence were designed specifically to deal with online communications.[80] However, the MCA is not entirely suited to harassment cases because the content of the communication needs to be 'grossly offensive' and not all behaviour which constitutes harassment will also be grossly offensive. It is clear, therefore, that the MCA is a useful tool against online communications. However, there are some issues which mean we need to be circumspect about both its ambit and its effectiveness in the context of cyberhate.

As mentioned above, the MCA is not an aggravated offence under the CDA. This means that even if a defendant is found guilty under the MCA, and he or she was motivated by or demonstrated hostility against the victim, this will not be taken into account at the offence stage of the offence, although it will be taken into consideration at the sentencing stage.[81] This does not sit well with the fact the CPS, in its guidelines, has pledged to take the 'hate' element in electronic communications more seriously, to the extent that a finding of hate may make a prosecution more likely than if it were a communication that were simply 'grossly offensive'.[82] The effect of this is that a perpetrator who sends out 1 racially abusive email to 1000 people will

---

79 https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2015 accessed 29 September 2017. Use the 'Outcome by Offence' table

80 Neal Geach and Nicola Haralambous, 'Regulating harassment: is the law fit for the social networking age?' (2009) 73(3) Journal of Criminal Law 241; see also Peter Coe, 'The social media paradox: an intersection with freedom of expression and the criminal law' (2015) 24 Information & Communications Technology Law 16, 39-40

81 We have very little knowledge of how the sentencing provisions are used, but the 5th cycle ECRI Report on the UK suggests that they are under-used and so not very effective at giving protection to hate - https://www.coe.int/t/dghl/monitoring/ecri/Country-by-country/United_Kingdom/GBR-CbC-V-2016-038-ENG.pdf accessed on 29 September 2017

82 See in particular the section entitled 'Category 4 - http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/#a09 accessed on 29 September 2017

be guilty of an MCA offence, which cannot be aggravated under the CDA, but if this same person sends that email twice to one person, then this could be prosecuted under the PHA which as a racially aggravated offence will carry a higher penalty. There is also the issue of labelling as it will mean the MCA offence will not carry the additional 'hate' label in the way that the aggravated PHA offence will. Furthermore, if, as seems to be the case, the CPS prefers to use the MCA rather than the PHA in some cases of online harassment, this is problematic for cyberhate offences because it means that the victim of an MCA offence will get less protection than the same victim under the PHA. This corroborates the point made earlier about the disjointed relationship between the different pieces of legislation, and reinforces the need to create a single coherent framework that is easier for the police and prosecutors to use.

Another important issue here relates to identifying the mischief of this offence. In order for a communication to come under the MCA, it has to be found to be 'indecent' or 'grossly offensive'. These terms are meant to be given their everyday meaning,[83] but the term 'grossly offensive' is problematic given that under the ECHR we do have the right to offend.[84] An important case in this context is *Connolly*, which involved a defendant who sent photos of aborted foetuses to pharmacists who were selling the morning after pill. He was convicted under the MCA, but appealed saying that being convicted on the basis that the photos were 'grossly offensive' went against his right to freedom of expression under Article 10 of the European Convention on Human Rights. The court, however, dismissed his appeal stating that 'grossly offensive' and 'indecent' do not go against his rights because a heightened meaning is given to those words by the courts, and that in any case, his convention rights do not justify him intending to cause distress or anxiety.[85]

Even if *Connolly* is correct on this point and the wording of the MCA is consistent with freedom of expression, the terms 'grossly offensive' or 'indecent' seem particularly outdated for such a modern problem. It is difficult to see how we can justify criminalising speech on the internet on the basis of 'gross offensiveness' or 'indecency'. When one considers the extent to which the incitement offences under the POA have very high thresholds in order to ensure no infringement of the right to freedom of expression, it is difficult to support, without deeper consideration, the existence of such a wide actus reus under the MCA which appears to give the state much more power to interfere with online speech.

---

83 *DPP v Connolly* [2007] EWHC 237 (Admin)
84 *Sunday Times v UK (No 2)* [1992] 14 EHRR 229
85 *DPP v Connolly* [2007] EWHC 237 (Admin); but see also Graeme Broadbent, 'Malicious Communications Act 1988: human rights' (2007) 71(4) Journal of Criminal Law 288

Paradoxically, whilst the wording of the actus reus of the offence is very wide, the mens rea required limits the ability of the law to deal with certain instances of cyberhate. The mens rea requires that the defendant intended to cause anxiety to whoever the communication was sent to or to whom he intends it to be communicated.[86] This would mean that a defendant who posts messages without this intention – perhaps because he/she is writing on a forum to like-minded people – then the offence is simply not made out. Whilst it could be argued that the wide actus reus is mitigated by the much narrower mens rea, if this narrowing means that the offence is limited in such a way that it cannot deal with certain types of harm, then the narrowing of the wide actus reus has occurred in the wrong way. This shows that whilst the MCA has been specifically designed to deal with online communications, it has not been created to deal with cyberhate, and as such, is not the ideal tool for protecting victims of online hate.

### 2) Communications Act 2003, s. 127(1) (hereafter "CA")

s.127(1) of the CA makes it an offence to send or to cause to be sent by means of a public electronic communications network a message (or other matter) that is grossly offensive or of an indecent, obscene or menacing character.

This offence has been increasingly used by the CPS for online offences.[87] In 2005, there were 355 prosecutions under s.127(1), and in 2015 there were 1,715. However, there are a number of problems with using s.127(1) to tackle online hate crime.

Firstly, as outlined above, the CA is not an aggravated offence under the CDA, and so any hate element perpetrated during the commission of this crime will not be recognised in the offence element.

Furthermore, it is clear from the case of *Collins* that the core of this offence lies not in the protection of victims, but rather in the need to safeguard the public communications system from being abused.[88] When this offence was originally conceived, the communications system was publicly funded, so arguably, this did make sense. Irrespective of any doubts about the

---

86 Malicious Communications Act 1988 s 1(1)(b)

87 https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2015 accessed on 29 September 2017. Use the 'Outcome by Offence' table

88 *DPP v Collins* [2006] UKHL 40; but see also Nick Taylor, 'Communications Act 2003: 'grossly offensive' message' (2007) 71(4) Journal of Criminal Law 301; Thomas Gibbons 'Grossly offensive communications' (2006) 11(4) Communications Law 136

historical reality of this,[89] it is certainly the case that the system is now privatised, so the rationale for creating such an offence has fallen away.[90] Either way, it is clear from the wording of the offence that it is not designed to protect the victims of the communication. In fact, there need be no victim. As with the MCA, this is a conduct crime where the actus reus of the offence lies in the making of the communication irrespective of whether it was ever received by anyone. Indeed, it is even wider than the MCA because there need be no intended victim either. Under the MCA you need to show that the defendant intended to cause someone anxiety or distress. All that is required under s.127(1) of the CA is that the defendant sends a message that is grossly offensive, indecent, obscene or menacing. The mens rea for this offence requires that the defendant knew or was aware that the content of their communication was grossly offensive, indecent, obscene or menacing.[91] This means that this would, for example, criminalise an online but private conversation between two racists on holocaust denial as the discussion could plausibly be characterised as 'grossly offensive'.[92]

This makes the offence very broad, and goes much further than the incitement to hatred offences which would only make such behaviour criminal if the comments were intended to stir up hatred or - in the case of racial hatred only - were likely to stir up hatred thereby. Thus, in the example given above of the two racists conversing privately over the internet, they are given the opportunity to argue that no stirring up of hatred was intended - it was just a discussion about how to interpret history; nor was hatred likely to be stirred up - it was a private conversation. The incitement offences also give the defendants a defence if the communication was made in a private dwelling and not heard or seen except by other persons in that or another dwelling, whereas no such defence exists under the CA. It is at least arguable that the racist holocaust deniers could claim this defence on the basis that both Ds made the comments in the privacy of their own home, and the conversation, whilst undertaken online, was not publicly available. Both these points mean that the CA offence is wider than the Part III offences. This is problematic as the incitement offences were designed as our unique hate speech laws, and were purposefully constructed to be of limited scope in order to comply with freedom of speech. The fact that the CA effectively criminalises online communications that would not fall within the

---

89 Thomas Gibbons 'Grossly offensive communications' (2006) 11(4) Communications Law 136
90 Alisdair A. Gillespie, 'Offensive Communications and the Law' (2006) 17(8) Entertainment Law Review 236
91 *Chambers v DPP* [2012] EWHC 2157 (Admin)
92 This point has been made a number of times: Nick Taylor, 'Communications Act 2003: 'grossly offensive' message' (2007) 71(4) Journal of Criminal Law 301; Alisdair A. Gillespie, 'Offensive Communications and the Law' (2006) 17(8) Entertainment Law Review 236; David Ormerod, 'Case Comment, Telecommunications: sending grossly offensive message by means of public electronic communications network' (2007) 1 Criminal Law Review 98

incitement offences if they were uttered offline seems to override this careful construction and highlights the problem of the fragmented and piecemeal nature of cyberhate laws.

The breadth of the offence and its potential for infringing freedom of expression, can also be seen in the fact that what is outlawed is communications that are 'grossly offensive' 'indecent' or 'obscene'. It is difficult to see how proscribing such words would come within the Art 10(2) exceptions, as it is unlikely to be seen as 'necessary in a democratic society' to outlaw communications simply based on their gross offensiveness, indecency or obscenity.[93] Trying to repress ideas or language simply because we do not like them is not sufficient within a liberal western democracy.

In fact, overbroad offences such as s.127(1) bring the law into disrepute. The infamous case of *Chambers*[94] is a good example of this. Paul Chambers was initially convicted of s.127(1) for tweeting a message saying 'Crap! Robin Hood Airport is closed! You've got a week and a bit to get your shit together otherwise I am blowing the airport sky high!!'. This was intended as an ongoing joke between him and his girlfriend, and was not intended to be menacing; and indeed was not taken to be menacing by the off-duty airport manager who eventually came across this message five days after it was tweeted. Chambers was originally found guilty of the offence, but was eventually acquitted two years after his original conviction by the Divisional Court. The CPS was criticised for even bringing this case, and Paul Chambers attracted a large level of support both from the general population but also from prominent public figures such as comedians Stephen Fry and Al Murray. As a result of this case, the CPS published their official guidelines on prosecuting cases involving communications sent via social media. Whilst these guidelines have been seen as a step forward[95] it is clearly unacceptable to have in existence an offence that is considered so broad that the CPS has to police itself. The principle of legal certainty requires that our laws are clear and give citizens the ability to regulate their lives. S.127(1) clearly breaches this. This serves to highlight once again the need for a much clearer articulation of the harm caused by cyberhate so that offences are both clear and certain, and come within the Article 10(2) exceptions.

**SECTION 2**

---

93 *Handyside v United Kingdon*, 24 Eur. Ct. H.R (ser A) (1976); *Éditions Plon v France* App. No 58184/00 ECHR 2004-IV, [42]. See also, *Sunday Times v UK (No 2)* [1992] 14 EHRR 229

94 *Chambers v DPP* [2012] EWHC 2157 (Admin)

95 Peter Coe, 'The social media paradox: an intersection with freedom of expression and the criminal law' (2015) 24 Information & Communications Technology Law 16; Jennifer Agate and Jocelyn Ledward, 'Social media: how the net is closing in on cyber bullies' (2013) 24(8) Entertainment Law Review 263

The discussion above has highlighted the shortcomings in the current legislation. Existing hate crimes are too narrow to encapsulate anything other than a limited category of instances of online hate, whilst the technology based offences appear to be either very wide so as to contravene basic rights to freedom of expression, or to not be victim-centred.

Before we go on to consider a framework for new online communications offences, two issues arising from the discussion above need to be considered in more detail. The first relates to whether or not we need targeted legislation in this area, or whether we can simply use offline offences with minor amendments. To answer this question, the harm caused by online hate will be explored in order to ascertain whether it differs from the harm caused by offline hate. A second issue that will be considered will be how the provisions under Article 10 of the European Convention on Human Rights will be addressed by any proposed legislation on online communications.

**Online and offline?**

One question that arises from the analysis of the current offences is the question of whether we need separate legislation to deal with online hatred, or whether we can use the already existing offences under the PHA and the POA. In the analysis above, it was found that whilst these offences can help protect some victims of hate, there are some obvious gaps because they were not designed to deal with online hate. Meanwhile, the offences that are designed to tackle online communications are both under and over-inclusive and do not appear to fit in with modern day notions about the harm caused by cyberhate. This next section aims to identify the ways in which the harm caused by online hate differs from that of offline hate, and to outline why we need separate targeted legislation to tackle it.

Whilst much online hate will be very similar in content and effect to offline hate,[%] the emerging research in this area suggests that there are differences that can have an impact on how we

[%] See for example the report by Galop which showed that much of the impact and consequences on victims of online hate is similar to the harm caused to victims of offline hate http://www.galop.org.uk/wp-content/uploads/2017/08/Online-hate-report.pdf accessed 29 September 2017. Harriet Fearn has also found that there is a big overlap between the harm caused by online and offline hate: *The Impacts of Cyberhate*, 2016, PhD thesis, Sussex University (found at http://sro.sussex.ac.uk/66869/1/Fearn%2C%20Harriet.pdf accessed 29 September

regulate this behaviour. For example, Fearn's research suggests that there is evidence that some victims of hate crime are less affected by online hate than offline hate, but that in extreme cases the consequences can in fact be more serious.[97]

There is, however, an additional harm caused by cyberhate due to the fact that these offences are committed on social media. This brings with it a 'public' element which is quite distinct even from the PHA offences. The 'public' element in the PHA offences is the threat to public order, whilst attacks broadcast on social media cause a harm that goes beyond the potential threat to public order, or even anxiety, harassment alarm or distress as encapsulated by the PHA offences. This additional harm is a reputational one because of the potential for public humiliation and embarrassment when comments appear on social media.

This is compounded by the fact that an attack carried out on the internet is potentially permanent in nature, and can have an almost limitless reach. Whilst there is no doubt that offline attacks can leave permanent scars and can cause immeasurable pain, the attacks themselves will usually be of a finite nature, and, once a perpetrator is caught, can be stopped. However, the permanency and reach of the internet can mean that online attacks never go away, even if a perpetrator is caught. This means that a victim of online hate can be at risk of being exposed to the attack time and time again, thus rendering thems re-victimised.

When viewing these three elements together – the publicness of the internet, its permanency and its reach – it can be seen that the victims of these attacks can be caused harm that goes beyond the damage caused by the words themselves. Citron has described several case studies of people who have been attacked and harassed viciously on the internet, and she has illustrated the impact this has had on their lives. As a result of comments and attacks made on social media, on discussion forums and on blogs, these women have lost their jobs, their relationships have broken down, and their lives have been torn apart.[98] The examples Citron cites show clearly how the impact these online attacks have had on the individuals concerned goes beyond the harm caused by the initial verbal attacks. The fact that these attacks have appeared on the internet, and are therefore publicly and permanently accessible to anyone have caused additional pain and harm.

---

2017). However, both also point out that there are also some differences in the experience of online and offline hate crime.

97 Harriet Fearn, *The Impacts of Cyberhate*, 2016, PhD thesis, Sussex University (found at http://sro.sussex.ac.uk/66869/1/Fearn%2C%20Harriet.pdf accessed 29 September 2017

98 Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014)

Furthermore, there is increasing evidence that online attacks of this kind can have an impact on victims' ability to maintain a public presence on the internet. Some of the victims interviewed by Citron found that the easiest way to avoid the harassment was to simply stop using the internet. However, this had a severe effect on their ability to pursue certain careers. For example, one of the women had hoped to become a journalist, but found that her attempts to write a blog – something that is now seen as a requirement for budding writers – simply attracted more attacks from the person who was harassing her.[99] Both Fearn and a recent report by Galop have found that victims of cyberhate will often change their online behaviour in order to avoid the attacks.[100]

Moreover, there is also increasing evidence that certain groups in society are more likely to attract hate when they have a prominent internet presence. The Guardian recently undertook data analysis of the abusive comments left by readers on the 'under the line' comments section of its website in order to evaluate the intensity of hate levelled at their journalists. Their research found that of the top 10 most abused journalists, 8 were women, and the other two were black men - one of whom was gay.[101] A study by Galop found that 84% of LGBT+ respondents had experienced more than one incidence of online abuse, and that online hate targeted at members of the LGBT community was often aimed at silencing them when they spoke about identity issues.[102] Thus, it seems to be increasingly clear that the hate perpetrated online is not equal, and some groups are suffering more than others. Paradoxically, offline hate crimes do not include gender as a protected characteristic. If the evidence suggests that women are particularly being targeted by online hate, then legislators need to give serious consideration to the inclusion of gender as a protected characteristic for any online offences.[103]

So far, this discussion has focussed on how these three distinctive elements of the internet – its publicness, its permanency and its reach – can cause harm to the individuals who are the target of the hate. However, these three features also demonstrate the fact that the harm caused by cyberhate extends beyond the individual, and can have a great impact on those who are

---

99 Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014)

100 http://www.galop.org.uk/wp-content/uploads/2017/08/Online-hate-report.pdf. Fearn has also found that there is a big overlap between the harm caused by online and offline hate: Harriet Fearn *The Impacts of Cyberhate*, 2016, PhD thesis (found at http://sro.sussex.ac.uk/66869/1/Fearn%2C%20Harriet.pdf accessed 29 September 2017)

101 https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments accessed on 29 September 2017

102 Melanie Stray 'Online Hate Crime Report 2017 – Challenging online homophobia, biphobia and transphobia' for Galop.org.uk http://www.galop.org.uk/wp-content/uploads/2017/08/Online-hate-report.pdf accessed 29 September 2017

103 Mark Austin Walters and Jessica Tumath, 'Gender "hostility", rape, and the hate crime paradigm' (2014) 77(4) Modern Law Review 563. See also Chara Bakalis 'The Victims of Hate Crime and the Principles of the Criminal Law' *Legal Studies* 2017 (early view online)

bystanders to that hate. Indeed, a great deal of cyberhate is not directed at any one individual in particular, but is often comprised of generalised comments directed at specified groups. There are three types of bystander that concern us here.

The first type, consists of those bystanders who observe the hate targeted at race, religion, gender, sexual orientation, transgender, disability, and who share those characteristics. Whilst research on this is in its infancy, there does appear to be evidence that these groups are affected by the level of hate targeted at their characteristic.[104] Awan and Zempi argue that unlike offline hate where threats of violence are often at the core of hate crime, in the virtual world, the hate speech aims to 'dehumanize and demonize' and 'relies on creating tensions'. [105] Their study has shown how Muslims exposed to negative generalised stereotypes about Muslims not only increased their feelings of vulnerability and fear of physical attacks in the offline world, but also leads to a perception of themselves as different, and leads to a disengagement with wider society. Fearn's research has also shown that the harm of cyberhate extends beyond the direct victim of cyberhate and that it can have a negative impact on those who witness it.[106] Awan and Zempi, and Fearn's work is very important as it corroborates the more theoretical discussions about the harm caused by hate speech. For instance, Waldron has likened hate speech to pollution that poisons the atmosphere, and acts as an obstacle to the full integration of minorities into mainstream society.[107] Thus, it can be seen that individuals are harmed by online hate speech even if they are not the direct targets of this hate.

Linked to this is a second type of bystander who comes across the hateful material, or who observes the unfolding hate on social media but is not themselves a member of the targeted group. Research by Fearn has found that unlike offline hate, the impact of online hate can be felt at similar levels by those who are *not* members of the targeted group as those who *are* members of the targeted group.[108] This is a very distinct type of harm, and confirms that the reach of cyberhate is more extensive than previously thought. This also suggests that the harm caused by cyberhate goes beyond the physical or tangible harms we usually associate with crime

---

104 Irene Zempi and Imran Awan *Islamophobia: Lived Experiences of Online and Offline Victimisation, (*Bristol: The Policy Press, 2016); Imran Awan and Irene Zempi "'I will Blow your face off'—*Virtual and Physical World Anti-Muslim Hate Crime'* 2017 (57(2) British Journal of Criminology 362; Imran Awan and Irene Zempi 'The Affinity between Online and Offline anti-Muslim Hate Crime: Dynamics and Impacts' (2016) 27 Aggression and Violent Behaviour 1.
105 Imran Awan and Irene Zempi "'I will Blow your face off'—*Virtual and Physical World Anti-Muslim Hate Crime'* 2017 (57(2) British Journal of Criminology 362
106 Harriet Fearn *The Impacts of Cyberhate*, 2016, PhD thesis (found at http://sro.sussex.ac.uk/66869/1/Fearn%2C%20Harriet.pdf accessed 29 September 2017) p 153
107 Jeremy Waldron *The Harm in Hate Speech* (Harvard University Press, 2012)
108 Harriet Fearn *The Impacts of Cyberhate*, 2016, PhD thesis (found at http://sro.sussex.ac.uk/66869/1/Fearn%2C%20Harriet.pdf accessed 29 September 2017)

and particularly hate crime, and in fact is linked to broader social principles such as that of equality.[109]

The third type of bystander of concern, is the bystander who might be influenced and even radicalised by their exposure to online hate. For example, Perry and Olsson (2009) have argued that the internet provides those who belong to groups we might broadly define as ones peddling 'hate' with the opportunity to 'retrench and reinvent … as a viable collective'.[110] It allows them to establish a collective identity and, Perry and Olsson argue, could potentially lead to a 'global racist subculture'.[111] The exchange of racist ideas can help normalise racist ideologies[112] by enabling perpetrators to morally disengage from the harm caused by racism.[113] Awan and Zempi have shown how victims of cyberhate have witnessed a mob mentality on the web, whereby one person can initiate the hate which is then replicated by bystanders who have observed the opening thread.[114] Thus, it can be seen that the harm of online hate speech extends to the normalisation of racism and the radicalisation of individuals to racist ideology.[115]

All these factors suggest that there is a distinctive element to the harm caused by online hate which the PHA and the POA are not able to capture. Moreover, this discussion further highlights the inadequacies of the CA and the MCA which focus on concepts such as 'gross offensiveness' and 'indecency' which seem to have little to do with the reality of the harm caused by online hate. Thus, a reformulation of the rules on online communications requires an overhaul of the existing regime with the creation of targeted cyberhate offences which are able to properly reflect the reality of the harm caused by cyberhate.

---

109 Chara Bakalis 'The Victims of Hate Crime and the Principles of the Criminal Law' *Legal Studies* 2017

110 Barbara Perry and Patrik Olsson, 'Cyberhate: the Globalization of Hate' (2009) 18(2) Information and Communications Technology Law 185

111 Barbara Perry and Patrik Olsson, 'Cyberhate: the Globalization of Hate' (2009) 18(2) Information and Communications Technology Law 185. See also Barbara Perry and Ryan Scrivens, '*White Pride Worldwide: Constructing global identities online*' in Jennifer Schweppe & Mark .Austin Walters (eds), *The globalization of hate: Internationalizing hate crime* (OUP 2016)

112 Jamie Cleland, Chris Anderson, C and Jack Aldridge-Deacon 'Islamophobia, war and non-Muslims as victims: An analysis of online discourse on an English Defence League message board' (2017) Ethnic and Racial Studies 1;

113 Nicholas Faulkner and Ana-Maria Bliuc *''It's okay to be racist': moral disengagement in online discussions of racist incidents in Australia'* (2016) 39 Ethnic and Racial Studies 2545

114 Imran Awan and Irene Zempi "'I will Blow your face off'—*Virtual and Physical World Anti-Muslim Hate Crime'* 2017 (57(2) British Journal of Criminology 362

115 For examples of the growing problem of online hate speech, see also James Banks, "Regulating Hate Speech Online" (2010) 24(3) International Review of Law, Computers & Technology 233; Yaman Akdeniz, 'Racism on the Internet' (Strasbourg, Council of Europe Publishing, 2009).

**Freedom of Speech**

The section above has argued that targeted cyberhate legislation is needed in this area. Given that any regulation of online hate by necessity requires the outlawing of words, it is necessary to outline the freedom of speech concerns in this area. This section will give an outline of the issues and will create a framework for understanding what will be required to ensure any existing or proposed provisions on online communications are compatible with our freedom of expression under Article 10 of the European Convention on Human Rights (hereafter 'ECHR').

Under Article 10(1) of the ECHR:

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

There are, however, exceptions to this which enable States to create legislation which curtails citizens' right to free speech so long as under Article 10(2) this is:

'…necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others…'.[116]

The European Court of Human Rights (hereafter "ECrtHR") has established a rich body of jurisprudence on Article 10 which outlines to what extent States can deviate from the basic principle of freedom of expression. This has established different levels of protection depending on the type of speech in question. Of particular interest here is the Strasbourg case-law on hate speech. A line of cases appears to have established a relatively low level of protection for speech deemed to incite hatred against minorities. For example, in *Pavel Ivanov v. Russia*[117] the applicant owned and edited a newspaper in Russia. He published a series of articles where he claimed that the Jews were the root of all evil in Russia. He was convicted of the offence of public incitement to ethnic, racial and religious hatred. He complained to the EcrtHR that his conviction was not justified. The court declared his application inadmissible because it said that such an assault against Jews was a fundamental attack against the Convention's underlying values: notably tolerance, social peace and non-discrimination, and therefore came within Article 17 which

---

116 See also *Handyside v United Kingdon*, 24 Eur. Ct. H.R (ser A) (1976) for a classic explanation of Article 10

117 *Pavel Ivanov v Russia,* Application no. 35222/04 (2007)

prevents the use of the Convention rights to 'engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms' in the Convention. Essentially, the Court was saying that the attack on Jews did not constitute 'speech', and thus did not engage Article 10 or its exceptions. This gives this type of speech very little protection, and gives State a very wide berth when it comes to criminalising such behaviour.

Indeed, such an approach was used in the case of *Norwood v UK*[118] where the applicant had displayed a BNP poster in his window with the Twin Towers in flames and the words 'Islam out of Britain – Protect the British People'. He was charged with s.5 of the POA, and complained to the Court that his right to freedom of speech had been breached. The court, however, said that the applicant could not use Article 10 to justify displaying the poster because the poster was a direct attack on the underlying values of the Convention, and so Article 17 was engaged which effectively disallowed him from any protection. This approach, in principle, does make the outlawing of hate speech a fairly simple matter from the point of view of freedom of expression. Very little scrutiny of the legislation itself will be undertaken by the ECrtHR as long as the legislation is only aimed at hate speech, and not at any other speech.

However, the issue is not as simple as this. As a matter of principle, the approach of the ECHR in relation to hate speech is by no means welcomed by all. There are many critics[119] who argue that this does not give sufficient protection to people's freedom of speech, and that subsequent case law has gone too far in using Article 17 as a way of excluding a proper discussion of whether the limitation was justified on its facts. Furthermore, the application of Article 17 has not been consistent.[120] Whilst it has been applied to ethnic hate,[121] racial hate[122], and religious hate,[123] a different approach has been adopted in relation to homophobic hate,[124] incitement to ethnic hatred[125] and incitement to racial discrimination or hatred[126]. In these cases, the ECHR has instead adopted an approach whereby the speech *is* found to engage Article 10, and so any legislation which prohibits such speech can only do so if the infringement can be justified under

---

118 *Norwood v UK* Application no. 23131/03 (2004)
119 See for example, Alex Bailin, 'Criminalising Free Speech?' (2011) 9 Criminal Law Review 705; Sophie Turenne, 'The compatibility of criminal liability with freedom of expression' (2007) Criminal Law Review 866; Tarlach McGonagle 'A Survery and Critical Analysis of Europe Strategies for Countering "Hate Speech"' in Michael Herz and Peter Molnar (eds), *The Content and Context of Hate* Speech (Cambridge University Press 2012)
120 Tarlach McGonagle, 'The Council of Europe against online hate speech: Conundrums and challenges' https://www.ivir.nl/publicaties/download/Expert_paper_hate_speech.pdf accessed 29 September 2017
121 *Pavel Ivanov v Russia,* Application no. 35222/04 (2007)
122 *Glimmerveen and Hagenbeek v the Netherlands* application nos. 8348/78 & 8406/78 (1979)
123 *Norwood v UK* Application no. 23131/03 (2004)
124 *Vejdeland and Others v Sweden* application no. 1813/07 (2012)
125 *Balsytė-Lideikienė v. Lithuania* Application no. 72596/01 (2008)
126 *Jersild v. Denmark,* 298 Eur. Ct. H.R. (ser A) (1994)

one of the exceptions under Article 10(2). This, therefore, requires the ECrtHR to give greater scrutiny to legislation involving these types of hate.

The picture within the ECHR is, therefore, not clear, and the level of scrutiny each piece of legislation will attract will depend on whether it is defined as pure hate speech or other type of hate speech. However, in the absence of a clear definition of what constitutes hate speech, as well as any clear justification as to the different levels of protection offered, it would be appropriate for the UK Parliament to take an approach which assumes that all hate speech legislation should be exposed to the higher level of scrutiny. Thus, the presumption would be that all hate speech engages Article 10, and so any incursion into freedom of expression needs to be justified under the Article 10(2) exceptions. This article will adopt this stricter approach to the issue of free speech and will recommend that any legislation on hate speech should only exist or be created where it can be shown that it is 'necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others.'

This means that the underlying purpose of each piece of legislation will need to be articulated and subsequently examined to determine whether the mischief it is protecting does indeed fall into the Article 10(2) exceptions. Furthermore, as *Handyside* has made clear, it is not just the legislation itself that needs to be compatible with Article 10. Each prosecution needs to be considered in light of the Article 10(2) exceptions. Therefore, contextual factors will need to be taken into account to determine whether each prosecution is necessary and proportionate. The CPS has already outlined a number of these factors in their Guidelines[127] such as whether effective action was taken to remove the communication from the internet or whether it was intended for a wider audience. This latter point is particularly important and will require a nuanced approach to material available online. Currently, offences such as the CA make no distinction based on how publicly available the communication is, and so can capture within it private comments. It is argued that any new legislation on online communication must contain guidance on how the context within which comments are made online can be important in determining the harm caused by that speech. It may be easier to justify the prohibition of speech where a comment has been made publicly such as on social media or in below the line comments of newspapers, than it would to prosecute comments made on a personal blog or in a private

[127] CPS guidelines on social media http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/ accessed on 29 September, see under under 'Art 10 ECHR' heading

email. Equally, it is necessary to accommodate the different way in which people converse online[128] as well as the level of thought and preparation that has gone into the speech.[129]

**Reform Proposals**

It has been established that the harm caused by cyberhate is distinctive in nature to that of offline hate, and requires separate targeted legislation. The discussion has also revealed that although the term 'cyberhate' is used to refer to online hate communications, it is clear that there are four different types of harm caused by online hate that emerge from the discussion above, and therefore separate legislation will need to be created to target these different types of harm.

- The first type of harm is the same harm caused by offline offences such as the POA and the PHA. This harm is caused to an individual when the harassment they experience takes place online but in a private form, through, for example, emails and text messages, and causes the same harm as offline behaviour, namely harassment, alarm or distress.
- The second type of harm is the additional harm caused to an individual when the hate is communicated on social media or another public forum. As well as harassment, alarm or distress, a victim in this scenario is likely to suffer additional reputational harm that may manifest itself in broken relationships, harm to career and an individual's ability to maintain a presence on the internet. This necessitates a different offence than the first type of harm in order to recognise this additional harm.
- The third type of harm covers the case of speech that is not directed at any one person in particular, but involves generalised hateful comments which poison the atmosphere and demonise particular groups of individuals who share a protected characteristic.
- The fourth type of harm is the potential radicalisation of individuals or the entrenching of global hate movements.

These different categories of offence can form the framework for a reformulation of the rules on cyberhate. It is important when regulating cyberhate to take separate account of each of these

---

128 Jones, B.C., '*The online/offline cognitive divide: Implications for law*' (2016) 13(1) SCRIPTed 83

129 Jacob Rowbottom 'To Rant, Vent and Converse: Protecting Low Level Digital Speech' 71(2) Cambridge Law Journal 355. See also more generally discussion by Alexander Brown 'What is so special about online (as compared to offline) hate speech?' Ethnicities, forthcoming, online first https://doi.org/10.1177/1468796817709846 accessed on 29 September 2017; Dominic McGoldrick, 'The Limits of Freedom of Expression on Facebook and Social Networking Sites: A UK perspective' (2013) 13 Human Rights Law Review 125. See also Big Brother Watch - https://bigbrotherwatch.org.uk/ accessed on 29 September 2017

categories, and so discrete offences will need to be created. Legislators will also need to give serious thought to including gender as a protected characteristic for online hate offences given that there is increasing evidence that women are particularly targeted by cyberhate speech.[130]

In legislating for these different categories of harm, several considerations present themselves. As a starting point, all legislation must be compatible with freedom of speech. It was argued above that it will be important in each case to articulate the mischief of the offence and to determine whether this makes the proscribing of speech necessary and proportionate in a democratic society. Thus, it will be important to delineate clearly what the actus reus and mens rea of these offences will be.

In relation to the first two types of harm, this is relatively straightforward if the focus is on creating result, rather than conduct crimes. Result crimes such as the PHA and the s.4A offence are easier to justify from a freedom of speech point of view than conduct crimes such as the incitement offences, the MCA or the CA because the harm caused can be more easily quantified – someone has been caused harassment, alarm or distress. If the offences in relation to the first and second harms outlined above are formulated as result crimes (albeit differently worded to the PHA and s.5), this will ensure they are compatible with freedom of expression. We need to move away using words such as 'gross offensiveness' or 'indecency' which do not reflect the harm being caused, but are also difficult to justify as being necessary in a democratic society. Focussing on the harm caused in these cases will obviate this difficulty.

However, when considering the third and fourth categories of harm, legislators will have to work harder to ensure these offences are compatible with human rights. This is because these offences will, by necessity, be conduct crimes. Whilst the justification for creating these offences is that they do cause the harms outlined above, the harm has not yet occurred and so the punishment needs to be proportionate to the actual risk. This will require the threshold of these offences to be higher in order to ensure consistency with freedom of expression. This could be achieved by requiring a high level of mens rea. However, the threshold will need to be slightly lower than the existing incitement offences which currently offer little protection to victims of online hate. Instead of a requirement that hatred is likely to be stirred up thereby, the emphasis

---

130 There is increasing evidence that women are particularly targeted online. See for example: https://www.demos.co.uk/press-release/staggering-scale-of-social-media-misogyny-mapped-in-new-demos-study/ accessed 29 September 2017; and https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments accessed on 29 September 2017

should be on prohibiting speech that is inconsistent with the values of contemporary society such as equality, tolerance, and community cohesion. The fourth category will focus on the need to show that the words are being used in such a way that they are liable to radicalise or influence others to engage in hatred of the protected characteristics.[131]

## CONCLUSION

The discussion above has shown how the current legislation on cyberhate is inadequate. It does not reflect the real nature of the harm caused by cyberhate and is not designed to tackle the particular problems associated with online hate. The fragmented nature of the current legislation also makes it difficult for prosecutors and the police to use.

An argument for creating separate offences that deal specifically with online hate was put forward and a framework for the creation of new cyberhate offences was proposed. It was argued that legislation needs to focus on four distinct types of harm caused by online hate: harm to individuals in a private forum, harm to individuals in a public forum, harm to vulnerable groups, and finally the harm caused to society by the radicalisation of others.

There is a level of urgency in relation to regulating cyberhate. The Working Group on Cyberhate, which was convened by the American Defamation League and which includes tech giants such as Facebook, Twitter, and Google as well as academics and industry experts, has met to co-ordinate industry standards on how to deal with hateful comments on social media. They have developed a code of conduct which is used by social media companies to set the standard of behaviour on their sites.[132] Whilst this is clearly a sign that the issue of cyberhate is being taken seriously, it is important to be cautious about allowing self-regulation to continue to develop in this way without some guidance from Parliament as to whether the parameters of good behaviour as determined by these tech giants accords with freedom of speech. For this

---

131 There is a debate in hate crime scholarship about the appropriate protected characteristics. See Neil Chakraborti and Jon Garland, 'Reconceptualizing hate crime victimization through the lens of vulnerability and "difference"' (2012) 16 Theoretical Criminology 499; Jennifer Schweppe 'Defining characteristics and politicizing victims: A legal perspective' (2012) 10 Journal of Hate Studies 173; Mohamad Al-Hakim, 'Making a home for the Homeless in Hate Crime Legislation' (2014) Journal of Interpersonal Violence 1; Gail Mason, 'Victim attributes in hate crime law: Difference and the politics of justice' (2014) 54 British Journal of Criminology 161; Chara Bakalis 'The Victims of Hate Crime and the Principles of the Criminal Law' *Legal Studies* 2017 (online); Michael Blake, 'Geeks and monsters: Bias crimes and social identity' (2001) 20 Law and Philosophy 121; Ryken Grattet and Valerie Jenness, 'Examining the Boundaries of Hate Crime Law: Disabilities and the "Dilemma of Difference"' in Barbara Perry (ed.), *Hate and Bias Crime: A Reader* (Routledge, 2003) 284;. It is suggested that the protected characteristics under the Equality Act should be used here.

132 https://www.adl.org/news/press-releases/adl-releases-best-practices-for-challenging-cyberhate accessed on 29 September 2017

reason, it is important to create clear rules on cyberhate in order to ensure that citizens and internet service providers are clear about the boundaries of appropriate online behaviour.