Written evidence submitted by
Chara Bakalis, Principal Lecturer in Law, Oxford Brookes University

The Legal Regulation of Online Hate

1. Executive Summary

- My overall proposition is that the existing legal regulation of online hate is insufficient to deal with the growing phenomenon of cyberhate. The legislation is too fragmented and does not properly capture the harm caused by hate on the internet. As such, it is too difficult for the police and prosecutors to use, hence the low number of prosecutions in this area.
- I will summarise some of the problems associated with the current legislation
- And will outline proposals for reform of the law and the creation of targeted cyberhate legislation

2. Problems with the Current Legislation

- The law is too fragmented. There are up to thirty different statutes which could potentially be used to punish online behaviour.
- However, despite a plethora of legislation that can be used in such situations, none of it is aimed specifically at tackling online hate.
  - If we focus on the four main pieces of legislation used, we can see that although some statutes are aimed at hate (Protection from Harassment Act 1998 and Public Order Act 1986), these are not designed to be used against online communications, and this can cause problems for prosecutors.
  - Meanwhile the offences which are designed to deal with online behaviour (Communications Act 2003 and Malicious Communications Act 1988) are not hate crime offences, and so the ‘hate’ element of the offending behaviour is not recognised within the offence itself. In addition to this, the wording of the Communications Act 2003, has led to the CPS creating its own guidelines on prosecuting social media communications as a way of limiting the potential wide application of the offence. This is not ideal as it should be Parliament who decides the limits of the offence.
- These offences also do not reflect the type of harm caused by online hate speech. There are a number of ways in which online hate differs from offline hate, and this means that separate offences targeted specifically at cyberhate are required:
  - The public element of an online hate crime distinguishes it from ordinary offline crime, and means that we need legislation that is able to reflect the extra harm caused by the broadcasting of the hate in the public sphere.
  - The potentially permanent nature of online hate, and the problems this causes victims of these sorts of attacks, also needs to be addressed by the law.
o There is increasing evidence that women seem to attract particular vitriol over the internet. However, gender is not currently a protected characteristic under the aggravated hate offences or the incitement to hatred offences. In addition to this, it is becoming increasingly clear that other minorities such as those of race, religion and sexual orientation are also targeted online. As these are protected characteristics under offline hate offences, online hate offences need to mirror this protection.

o The freedom of speech questions which inevitably arise in this area need to be considered in the context of the online world. Our current legislation relies on adopting a balance between freedom of speech and protecting the victims of hate based on an offline vision of the world. The online world requires us to reformulate the limitations on free speech which recognises the increasing presence of the internet in our lives.

o There are also practical issues that make the prosecution of online hate different to offline hate.
  - It is not always easy to identify or track down the offender of online hate. We need legislation that would require ISPs to hand over the contact details of those who use their services and are suspects of crime.
  - In addition to this, more domestic powers need to be created which would allow for offending behaviour to be removed entirely from the internet, or at least to compel search engines, such as Google, to remove such material from their searches (see for example Google Spain).

3. Potential Reform proposal

My main contention is that we need targeted offences at cyberhate as online hate needs to be treated separately from ordinary real life hate crimes. There is also tendency to view cyberhate as an amorphous mass which includes any hate speech that is perpetrated over the internet. However, we need legislation that is targeted at the different types of harms caused. Separating out the different harms in this way, is also beneficial insofar as freedom of speech is concerned. It will enable us to find a balance between freedom of speech and the protection of victims that is flexible, taking into account the different contexts within which harm is caused.

  o We need to divide the types of harm caused by cyberhate into four different categories.
    - The first type of harm, is targeted hate against a particular individual which takes place online, but in a private way. Perhaps through email or comments on blogs that the victim is able to delete themselves. This is would be akin to harassment.
    - The second type of harm also involves the targeting of an individual, but where this is done in a public way. An example of this would be hateful comments posted on social media or in public discussion forums or on comments sections of newspapers.
The third type of harm is **public defamation against a group**. This is where a group has been publicly attacked in some way.

The final category is **propaganda that is targeted at like-minded individuals**. This is more akin to incitement to hatred offences but also has an element of ‘grooming’ to it. Barbara Perry and Ryan Scrivens who are Canadian academics have shown how, for example, white pride groups use the internet as a way of constructing a global white supremacist identity. The law in the UK on incitement has a very high threshold, and it is very hard to get successful prosecutions under this even for non-cyberhate cases, so this high threshold may need to be re-thought given the likely greater harm that might result from online hate.

In addition to this we also need:

- Clearer rules on the duty of ISPs to hand over information required by the police, and the responsibility to remove criminal material from the internet insofar as is possible.

There is a level of urgency when it comes to legislating on cyberhate. A key to the success of any legislation in this area is international collaboration, simply because many internet service providers are located in the US, and so co-operation with America on this is crucial. However, this is very difficult to achieve because American law gives (or at least is thought to give) far greater protection to free speech than we do in Europe, and so US companies based in the US can simply refuse to comply with rulings of European courts on these issues if they believe that they infringe free speech. As a way of overcoming this problem, the American Defamation League (ADL), have convened a working group on cyberhate that includes tech giants like Facebook, Twitter, Google, Yahoo, Microsoft, YouTube as well as academics and industry experts who have met to coordinate industry standards on how to deal with hateful comments. This shows progress in this area. However, we need to be cautious about allowing self-regulation to continue in this way without some guidance from the law. This is because whilst it is surely a good thing that Facebook and Twitter are taking seriously the issue of online hate, it should be Parliament that decides what the appropriate parameters of free speech should be – and not Silicon Valley. In order to ensure that these companies are not under or over-policing our free speech, we need Parliament to tell us – in the form of cyberhate legislation - what the correct balance is between freedom of speech and protecting vulnerable victims of cyberhate.

**Chara Bakalis, Principal Lecturer in Law, Oxford Brookes University.**

*My specialism is hate crime and cyberhate.*