European regulation of cross-border hate speech in cyberspace: The limits of legislation

BANKS, James <http://orcid.org/0000-0002-1899-9057>

Available from Sheffield Hallam University Research Archive (SHURA) at:
http://shura.shu.ac.uk/6902/

This document is the author deposited version. You are advised to consult the publisher's version if you wish to cite from it.

Published version


Copyright and re-use policy

See http://shura.shu.ac.uk/information.html
European Regulation of Cross-Border Hate Speech in Cyberspace: The Limits of Legislation

James Banks

Department of Law, Criminology and Community Justice, Sheffield Hallam University, Sheffield, England.

1. Introduction

As an egalitarian communications medium, the Internet has the ability to cross borders, destroy distance and break down real world barriers. Globalised, decentralised and interactive, the computer network offers a technological landscape largely unfettered by governmental regulation, which could obstruct the free flow of knowledge, ideas and information. However, the dramatic growth of the Internet has been accompanied by increased governance of content and behaviour by state, public and private actors. More recently, European states' criminalisation of the publication of hate propaganda has been followed by efforts to prosecute individuals for the dissemination of racist and xenophobic material online.

This paper examines the complexities of regulating hate speech on the Internet through legal frameworks. It demonstrates the limitations of unilateral national content legislation and the difficulties inherent in multilateral efforts to regulate the Internet. The paper highlights how the US's commitment to free speech has undermined European efforts to construct a truly international regulatory system. It is argued that a broad coalition of citizens, industry and government, employing technological, educational and legal frameworks, may offer the most effective approach through which to limit the effects of hate speech originating from outside of European borders.

---

3 Austria, Azerbaijan, Belgium, Bosnia, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Ireland, Italy, Lithuania, The Netherlands, Norway, Romania, Russia, Serbia, Sweden, Switzerland, The United Kingdom.
2. Hate Speech

2.1 Definitions

Hate speech is a contested concept with states, academics and private companies providing varying definitions. For example, Coliver highlights how: 'Hate speech' and 'hate expression' refer to expression which is abusive, insulting, intimidating, harassing and/ or which incites to violence, hatred or discrimination…based on that person's identification with a group on such grounds as 'race, ethnicity, national origin or religion'.⁴ Weintraub-Reiter broadens this definition to include '[o]ffensive, racist, hate-laden speech that disparages racial, ethnic, religious or other discrete groups, including women, lesbians or homosexuals.⁵ What is evident is that the concept of 'hate speech' is constantly evolving:

Traditionally it included any form of expression deemed offensive to any racial, religious, ethnic, or national group. In the 1980s some campus speech codes broadened it to include gender, age, sexual preference, marital status, physical capacity, and other categories. Human Rights Watch defines hate speech as 'any form of expression regarded as offensive to racial, ethnic and religious groups and other discrete minorities, and to women.' Rodney Smolla defines it as a 'generic term that has come to embrace the use of speech attacks based on race, ethnicity, religion and sexual orientation or preference.' Historically, hate speech has been referred to by several terms. In the late 1920s and early 1930s it was known as 'race hate.' Beginning in the 1940s it was generally called 'group libel', reflecting the specific legal question whether the law of libel should be expanded to cover groups as well as individuals. In the 1980s 'hate speech' and 'racist speech' became the most common terms.⁶

Nevertheless, the vast majority of academic discussion of online hate speech has focused upon racist and xenophobic material.⁷ For the purpose of this paper, discussion will focus on the regulation of racist and xenophobic online content.

---

⁵ R. Wentraub-Reiter, 'Note: Hate Speech over the Internet: A Traditional Constitutional Analysis or a New Cyber Constitution?, Boston Public Interest Law Journal, 8 (1998), 145.
⁶ S. Walker, Hate Speech: The History of an American Controversy (Nebraska, University of Nebraska, 1994).
2.2. How much Hate?

The anonymity, immediacy and global nature of the Internet have made it an ideal tool for extremists and hatemongers to promote hate. The globalisation of technology has been accompanied by an incremental rise in the number of online hate groups and hate related activities taking place in cyberspace. With computers becoming less expensive, simpler to use and more readily available, the opportunity for bigots to utilise modern day technology to spread their propaganda has increased. Inexpensive and unencumbered, the Internet has become the 'new frontier' for spreading hate. With millions reached in seconds, the Internet offers a social network that enables previously diverse and fragmented groups to connect, engendering a collective identity and sense of community. Consequently, an online 'global racist subculture' has replaced previously isolated and atomised members of far-right parties.

The peripatetic nature of hate sites makes accurate quantification extremely difficult. Nevertheless, attempts to quantify the problem suggest that the number of such sites is growing at an alarming rate. White nationalist and former Ku Klux Klan member, Donald Black, launched the first extremist website, stormfront.org, in April 1995. Since then the number of hate sites has ballooned. Early attempts at quantification suggested that 'Hi-Tech Hate' was spreading rapidly. Perry's first paper on the hate movement identified approximately 120 hate sites in existence by 1997, whilst the Anti-Defamation League (ADL) estimated that the number of hate sites stood at around 250. At the turn of the century, it was recorded that the number of hate sites had grown to around 400. A decade later, the number of hate sites in existence is said to stand at a staggering 8,000.

---

12 Perry and Olson, Cyberhate: the globalization of hate’, 190.
13 Ibid; Simon Wiesenthal Center, Digital Terrorism and Hate 2.0 (Los Angeles: SWC, 2008).
14 Anti-Defamation League, Hi-tech hate: Extremist use of the Internet.
16 Anti-Defamation League, Hi-tech hate: Extremist use of the Internet.
17 B. Levin, 'Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America', American Behavioural Scientist, 45, no.6 (2002), 958-988.
18 Simon Wiesenthal Center, Digital Terrorism and Hate 2.0.
Racists and far-right extremist groups have also begun to utilise social networking sites such as Facebook and Myspace to spread their propaganda.\textsuperscript{19} With over 200 million users, social networking sites offer extremists an important platform upon which to espouse their ideas and beliefs, educate others and mobilise for demonstrations and rallies. Unsurprisingly: 'As more and more people are going to MySpace, YouTube, and especially Facebook, the extremists...they're going to exactly the same neighbourhood'.\textsuperscript{20} Websites, private message boards, listservs and email have also enabled extremists and hatemongers to propagate their rhetoric and strategies, recruit, organise and unify.

Moreover, the protection afforded by the Internet means that 'a perpetrator of a threat or harassing speech need not be at the actual scene of the crime (or within 5,000 miles, for that matter) to prey on his or her victim'.\textsuperscript{21} The rise in web-based hate speech, harassment, bullying and discrimination has mirrored the growth in online hate groups, with individuals targeted directly and indirectly through forums, blogs and emails.\textsuperscript{22} Limited policing of hate speech online has enabled such activities to flourish as criminal justice agencies are unable or unwilling to dedicate time and money to investigate offences that are not a significant public priority. As such, the police will rarely respond to online hate speech unless a specific crime is reported. Nevertheless, despite such shortcomings, more and more nation states have sought to legislate against the publication of hate propaganda and hate speech online.

3. The Limits of European State Based Regulation

Despite the geographic indeterminacy of the Internet, European states have sought to impose virtual borders onto cyberspace in order to regulate online hate speech. However, limited jurisdictional reach and conflict that has occurred when states have sought to enforce laws extraterritorially into other jurisdictions has stymied efforts to legislate against offensive material online. This may be considered unsurprising given that national laws on hate diverge so widely, as a consequence of countries unique historical, philosophical and constitutional

\textsuperscript{19} MailOnline, Facebook campaigners call for tougher controls on racist 'cyberhate' groups, available at http://www.dailymail.co.uk/news/article-1172799/Facebook-campaigners-tougher-controls-racist-cyberhate-groups.html (12 November 2009).
\textsuperscript{22} Perry and Olson, 'Cyberhate: the globalization of hate', 190.
traditions in relation to freedom of expression.\textsuperscript{23} Most notably, the US First Amendment affords considerable protection to those espousing hate from American websites, in direct contrast with many other nations' approach to hate speech.\textsuperscript{24}

The shift towards nation states imposing geographical demarcations onto the virtual world and the difficulties inherent in European countries seeking to extend their jurisdiction extraterritorially, enforcing their content laws against material uploaded beyond national boundaries, is exemplified in the case of Yahoo!.

In Yahoo!, Inc v. La Ligue Contre Le Racisme et L'Antisemitisme, two French student organisations alleged that Yahoo! had violated Article R. 645-1 du Code Penal, by displaying Nazi memorabilia on its auction website, and sought to prosecute the Internet Service Provider (ISP) for contravening French law. Article R. 645-1 du Code Penal outlaws the wearing or public display of insignia, emblem or uniform of an organisation or individual responsible for crimes against humanity, as such behaviour is deemed to be a serious crime 'against the people, the state and public safety'.\textsuperscript{25}

As the content originated in the United States, where such conduct is protected by the First Amendment, Yahoo! argued that its actions lay beyond French territorial jurisdiction. Dismissing this claim, Judge Jean-Jacques Gomes ruled that Yahoo! were liable and should seek to "eliminate French citizens' access to any material on the Yahoo.com auction site that offers for sale any Nazi objects, relics, insignia, emblems, and flags."

Gomes applied an effects-based jurisdictional analysis, granting prescriptive jurisdiction and ruling that intentional transmission, in addition to the local impact of the visualisation of Nazi memorabilia, provided sufficient grounds for finding jurisdiction. Highlighting how geo-location technology, combined with a declaration of nationality from service users, could filter out up to 90 per cent of French citizens, Gomes ruled that Yahoo! apply such mechanisms in order to seek to reduce access to the sale of Nazi merchandise. Failure to comply with the court order within three months would result in Yahoo! becoming subject to a penalty of 100,000 francs per day.

\textsuperscript{24} Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.
\textsuperscript{25} La Ligue Contre La Racisme et L'Antisemitisme (LICRA) and Union Des Etudiants Juifs De France (UEJF) v. Yahoo! Inc. and Yahoo France. English translation available at http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm (5 February 2010).
\textsuperscript{26} Ibid.
In response, Yahoo! sought and received, from the United States District Court for the Northern District of California, a judicial ruling that the enforcement of the French court's decision would breach the First Amendment of the Constitution. The US court declared that unless it could be demonstrated that such speech contains a direct, credible 'true' threat against an identifiable individual, organisation or institution; it meets the legal test for harassment; or it constitutes incitement to imminent lawless action likely to occur, it would be protected under the First Amendment. District Judge Jeremy Fogel ruled that the enforcement of foreign judgement is founded upon a "comity of nations", and that the court could not "enforce a foreign order that violates the protections of the United States Constitution by chilling protected speech that occurs simultaneously within our borders." On appeal, the Ninth circuit ruled that as there was insufficient contact between La Ligue Contre Le Racisme et L'Antisemitisme and L'Union des étudiants juifs de France and the forum state there was no basis for jurisdiction.

An alternative reason for issuing the declaratory judgement was made in an amici curiae brief to the United States Court of Appeals for the Ninth Circuit by the United States Chamber of Commerce and a number of industry associations. It stated that Yahoo! was an American company that "provides Internet services in English, targeted at American citizens, from host computers located in the United States" and that the French court had no jurisdiction. The brief highlights how the Yahoo! website does not meet the requirement of the "minimum contacts" test for jurisdiction, which states that "the maintenance of a passive website does not, as a matter of law, demonstrate that the corporation has 'purposefully (albeit Electronically) directed his activity in a substantial way to the forum state.'" The brief reiterated the United States District Court for the Northern District of California's judicial ruling that enforcement would have a chilling effect on free speech: "Faced with the fear of such prosecution, companies and individuals would inevitably feel pressured to remove

28 Yahoo! Inc. V. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d at 1192("The extent to which the United States, or any state, honours the judicial decrees of foreign nations is a matter of choice, governed by 'the comity of nations.'" (quoting Hilton v. Guyot, 159 U.S. 113, 163 (1895))).
29 Ibid.
30 Yahoo! Inc. V. La Ligue Contre Le Racisme et L'Antisemitisme, 379 F.3d 1120, 1123 (9th Cir. 2004).
31 Blarcum, Internet Hate Speech.
32 Brief Amici Curiae of Chamber of Commerce of the United States et al., Yahoo! Inc. V. La Ligue Contre Le Racisme et L'Antisemitisme, at 20 (9th Cir. 2002) (Case No. 01-17424) (quoting Cybersell, Inc v Cybesell, Inc., 130 F.3d 414, 418 (9th Cir. 1997)) (emphasis added by brief).
material that might be unlawful in any jurisdiction, thus giving the most restrictive
domestic laws in the world de facto veto over the content available."

The cultural tension inherent in attempts to regulate online speech extraterritorially is
evidenced in the case of Yahoo!. As Fagin recognises: ‘The standoff between America’s
indirect unilateralism and the European response rooted in effects-based jurisdiction is
unlikely to promote the overall collective good; instead we should favour the technical
evolution of the medium as a collaborative enterprise.’ The failure of states to extend the
reach of national laws beyond their borders means that hate speech which originates in one
jurisdiction, but whose effects are felt elsewhere, continue to go unregulated. Hate crime
offenders are, therefore, free to thwart the somewhat arbitrary assemblage of national laws
and evade identification and prosecution.

To address such failings, the Council of Europe have introduced a protocol aimed at
harmonising national legal system's computer related offences in order to reach a common
minimum standard of relevant offences and enable cooperation in the prosecution of those
committing hate crimes in cyberspace. Discussion now turns to examine this provision.

4. The Council of Europe's Convention on Cybercrime: Towards International
Harmonisation?

Formed in 1949, the Council of Europe has grown from ten founding members to forty-seven
member states as of 2010. Charged with securing democracy and preventing human rights
abuses, the Council promotes intergovernmental coordination and cooperation through the
passage of treaties. However, treaties have no legal effect unless they are both signed and
ratified by member countries.

The Council of Europe's Convention on Cybercrime is the first multilateral compact
that seeks to combat computer based crime by harmonising the national laws and
investigatory techniques of European nations. Whilst non-European countries are prevented
from membership of the Council, many have observer status and they are often invited to sign
and ratify council treaties in order to broaden the scope and impact of provisions. The
Convention on Cybercrime, which provides a multilateral framework for tackling a variety of
Internet crimes, including child pornography, copyright infringement and fraud, has been

33 Ibid at 11.
34 M. Fagin, Regulating Speech Across Borders: Technology Vs. Values, available at
35 Council of Europe, ‘Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of
acts of racist and xenophobic nature committed through computer systems, CETS 189’, available at
both signed and ratified by the US. However, their signature was only secured after an
Internet hate speech protocol, which was initially included in the original draft of the
Convention, was removed because it was deemed inconsistent with their constitutional
guarantees.

Introducing a separate protocol to address hate speech online, the Council of Europe
required signatories to criminalise acts of a racist and xenophobic nature committed through
computer systems. Under the protocol:

'racist and xenophobic material' means any written material, any image or any
other representation of ideas or theories, which advocates, promotes or incites
hatred, discrimination or violence, against any individual or group of individuals,
based on race, colour, descent or national or ethnic origin, as well as religion if
used as a pretext for any of these factors.

Alongside criminalisation of such material, the protocol extends the scope of the
Convention's extradition provision to include those sought for Internet hate speech crimes.

By the start of 2010, the Additional Protocol to the Convention on Cybercrime, had
been signed by 32 member states and ratified by 15. The US has, however, informed the
Council that it will not be party to the protocol as it runs counter to the First Amendment of
its Constitution. As most hate sites originate in the US, their commitment to indirect
unilateralism is extremely problematic. The US has no bilateral extradition treaties with
European countries and, therefore, no commitment to deliver defendants to be charged with
committing hate speech offences. With European countries both unable to extradite American
offenders for criminal prosecution and powerless to enforce civil judgements in American
courts, the US offers a significant safe haven for those propagating hate. Shutting down a
web site in Europe doesn't necessary result in permanent censorship. Prosecuting Internet
hate speech or closing a web site in one country may be futile if the individual can post from,
or material can reappear on a web page hosted by, an Internet Service Provider in the US.

36 Council of Europe, 'Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of
acts of racist and xenophobic nature committed through computer systems, CETS 189, List of Signatories’,
available at
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=17/02/2006&CL=ENG (11
February 2010).
37 Blarcum, Internet Hate Speech.
38 C. Wolf, 'Hate speech on the Internet and the law', available at http:adl.org/osce/osce_legal_analysis.pdf (5
February 2010).
Whilst the Additional Protocol is a laudatory endeavour, it is undoubtedly limited in its ability to bring together real differences in the ways in which states envisage hate speech and construct a legal framework through which hate based conduct may be reduced. The European Council's efforts to combat online hate speech are undermined by the US First Amendment which provides a safe haven for many of those propagating hate. With transference rather than prevention the likely outcome of increased legal regulation, cooperation and coordination amongst the European community, the law alone may not be the most appropriate mechanism through which to counteract hate speech online.

5. Beyond the Legal Regulation of Hate Speech in Cyberspace

As Perry and Olsson correctly note: 'The law is not the only - or perhaps even the most effective - weapon available to counter cyberhate'. As detailed above, the difficulties inherent in unilateral and multilateral legal regulation of the Internet limit European nation’s effective governance of online hate. As such, recourse to technological regulation, at both user and server ends, alongside the education of web users, may be deemed a more effective approach through which to minimise both the transmission and reception of online hate speech.

5.1 Internet Service Provider Self-Regulation

Internet Service Providers can play a central role in limiting Internet user's access to, and the effects of, harmful content. Codes of conduct or Terms of Service (TOS) agreements allow ISPs to screen hosted content and remove harmful or offensive material that breaches their policies. Consequently, ISPs are able to delete content, or cancel their service, if users fail to operate within TOS agreements.

A number of ISPs have actively sought to regulate hate speech, remove offensive material from their servers and shut down extremist sites. For example, America Online deleted a neo-Nazi Website, the Nationalist Online, from its server for violating its terms of service agreement, which prohibits content that is racially or ethnically offensive. In the UK and Germany, ISPs have formed industry organisations, which have developed codes of conduct prohibiting hate speech. For example, the Code of Practice of the Internet Service Providers Association (ISPA) of the United Kingdom sets down clear guidelines for British ISPs that requires members to 'use their reasonable endeavours to ensure… services and

39 Perry and Olson, 'Cyberhate: the globalization of hate', 196.
promotional material do not contain child abuse images or material inciting violence, cruelty or racial hatred.\textsuperscript{40}

Voluntary codes of conduct, to which customers must consent, offer an important mechanism through which to regulate websites originating in the US as they circumvent the First Amendment. However, in the US there are no industry wide regulatory bodies and the vast majority of the many thousands of access providers do not regulate against hate speech per se. Many TOS agreements are extremely narrow in focus, so whilst libellous or defamatory speech is prohibited, they do not extend to those acts that fall within the First Amendment’s free speech protections. Under Section 230 of the Communications Decency Act, ISPs cannot be held criminally responsible for the content of the sites they host. There is, therefore, little motivation for ISPs to self regulate. Moreover, as removal tends to be contingent on commerciality and cost, many ISPs do not have the desire or means through which to address harmful content. Consequently, as the vast majority of hate sites are hosted in the US, ISP based technological regulation has serious limitations for European nations.

5.2 Filtering
Alternatively, European governments can seek to block extraterritorial websites that do not comply with their national laws. Spain are one country that have undertaken such an approach, passing legislation which authorises judges to shut down Spanish sites and block access to US based web pages that do not comply with national laws.\textsuperscript{41} The implementation of geographic location technology can further enable both servers and states to control the flow of information on the Internet through the identification of users IP address, which can be used to both restrict access and filter out odious material.

Private users can also employ software, such as firewalls, to filter out sites containing certain speech. Numerous commercial Internet filtering software packages are readily available and can easily be installed on computers. For example, in 1998, ADL introduced Hatefilter, a filtering software product that not only prevents access to websites that promote hate but also educates users about the nature of bigotry and why such sites should be rejected.\textsuperscript{42} Similarly, Surfwatch blocks hate speech, alongside gambling sites and sexually

explicit content, whilst Bess and CyberPatrol also offer filters which bar access to anti-Semitic, racist, and other forms of hate speech.

5.3 Education
Individual responses to online hate may only have a limited impact on access to online material but the responsibilisation of individual users can both promote a culture of intolerance towards online hate and contribute to efforts to 'reclaim' the web. ADL, the Simon Wiesenthal Center and the Southern Poverty Law Center have undertaken a number of high profile educational campaigns that have sought to make the public aware of online hate and provide them with strategies through which to combat such materials. For example, ADL have authored a parents guide to hate on the Internet, 'Helping Your Child Safely Navigate the Information Superhighway', which encourages parents to help their children deal with online hate through discussion and education.

5.4 Monitoring
Users can also play an important role in monitoring Internet content and alerting relevant authorities to incidents of cyberhate that may warrant law enforcement intervention. Hate speech hotlines have become an effective means through which citizens can alert ISPs to material that breaks their codes of conduct, or law enforcement agencies to sites or incidents of cyberhate which may warrant investigation and prosecution. Monitoring organisations, such as the ADL and Simon Wiesenthal Center, continue to work closely with ISPs in identifying and removing hate based websites and messages and materials that contravene TOS contracts. ADL also seek to highlight material that is harmful in content and have been particularly successful in providing the public with information concerning online hate materials. In 2004, Google responded to a ADL’s concerns about access to anti-Semitic Website 'Jew Watch' by introducing an 'offensive search results' link that explains why some extremist websites appear in users search findings. More recently, YouTube has introduced an ADL authored guide on tackling hate speech in its Abuse and Safety Centre.

6. Conclusion
The exponential growth of the Internet as a means of communication has been emulated by an increase in far-right and extremist web sites and hate based activity in cyberspace. The

anonymity and mobility afforded by the Internet has made harassment and expressions of hate effortless in a landscape that is abstract and beyond the realms of traditional law enforcement. European states have sought to regulate the domain of the Internet through the conventional strategy of national law. However, the multi-jurisdictionality of the Internet has undermined their efforts to place geographical demarcations onto cyberspace.

With unilateral attempts to regulate hate speech originating in foreign territories falling foul to jurisdictional and cultural conflict, the application of national law to foreign entities has serious limitations. Therefore, an international system governed by compacts and supranational decision making would appear to offer an appropriate means through which to obviate regulatory conflict between nation states. Yet, the Council of Europe's collaborative enterprise has been seriously undermined by the US's commitment to free speech. So whilst the US approach to regulation has become a minority view, its indirect unilateralism detracts from European efforts to construct a truly international regulatory system. The US, therefore, continue to provide a suitable safe haven for many of those transmitting hate.

Unilateral and multilateral efforts to regulate online through criminal law alone will not be enough to reduce the effects of online hate. The episodic prosecution of individual web users is unlikely to deter others from posting hate speech online. Web sites that are closed in one jurisdiction may simply re-open in another thus remaining available to Internet users worldwide. Furthermore, the global nature of the Internet makes the total legal regulation of cyberspace impossible. Consequently, it is necessary to seek alternatives through which to both limit the publication of hate speech online and minimise the harm caused by such behaviour.

By combining legal intervention with technological regulatory mechanisms – monitoring, IPS user agreements, user end software and hotlines – the harm caused by online hate can be diminished. Moreover, through the careful integration of law, technology, education and guidance, a reduction in the dissemination and impact of online hate speech can be achieved without adversely affecting the free flow of knowledge, ideas and information online. As Bailey neatly summarises, "broad-based efforts involving strategic alliances among citizens, citizen coalitions, industry and government provide a strong foundation from which to engage in visible, publicly accountable action against cyberhate."\(^{44}\) For such an alliance to operate effectively, governments, businesses and citizenry must all engage in individual and collective solutions to minimising online hate speech.

\(^{44}\) Bailey, Strategic Alliances, 58.