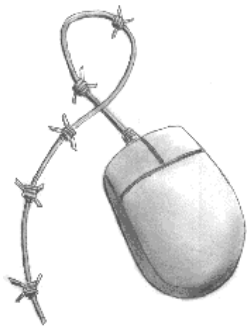
GreenNet CSIR Toolkit Briefing no. 9



Expression and Defamation

Your rights to free speech online, and when free speech transgresses the boundary of defamation

Written by Paul Mobbs for the
GreenNet *Civil Society Internet Rights Project*, 2002.
http://www.internetrights.org.uk/

It is accepted in a democratic society that individuals have a right to express their own views and preferences. Democratic states also accept that individuals have rights to some degree of privacy, to protect their reputation and to prevent the dissemination of false or inaccurate information about them. The balance that is struck between these rights has crucial importance for the Internet, as do the conflicts that can arise in the course of that balancing act.

The Internet, of course, offers extensive potential for individuals and organisations to broadcast or publish information. A key aspect is the facility it gives people for associating with others and expressing views openly. That potential is coming under increasing pressure from governments and security organisations who are keen to have all Internet transactions monitored.

The issue of defamation lies on the other side of the coin from free speech, and is therefore also a central issue in the use of the 'Net. It is important to ensure that unfounded claims do not damage people's reputations, lives or careers. Some corporations, however, now use the threat of a legal action for defamation as a means to restrict the actions of groups or individuals campaigning against their activities[1].

Rights of expression and protection from defamation are closely linked to issues of personal privacy. Prior to the Human Rights Act 1998, there was no right to privacy under UK law. The Internet has various mechanisms for monitoring the use of services, and the information transmitted; in the online world, the protection of privacy is as important as protecting rights to free expression and protection against defamation.

The right of expression

Exercising the right of expression on the Internet is a complex business, and it is a right that is all too easily ceded in everyday use. This use can involve transactions covering a number of geographical locations, each, potentially, with a different legal framework and standards for protecting rights to expression. These rights can quite easily be violated; ownership of the Internet is in the hands of private companies, for the most part, and the contractual obligations most people agree to when arranging Internet access give the system operator the right to restrict or prevent contact and communication with others in certain ways.

In Europe rights to freedom of expression and association are guaranteed under Articles 10 and 11 of the

[1]For a detailed account of how the law is used as a means of repression by certain corporations see the book *Green Backlash* by Andrew Rowell (Routledge, 1996)

European Convention on Human Rights[2]. Some countries have their own legal traditions and frameworks that either augment the Convention or, as in the case of rights to expression under the American constitution, for example, protect personal expression according to other principles. These differences, and especially the difference between European and US models, lead to some of the greatest debates on use and abuse of the Internet. Recent concerns about the use of the Internet to promote anti-Semitic or racially motivated hate, or to permit the divulgence of personal information via web sites, are all related to the conflict between the European and US models of 'freedom of expression'. This conflict has even wider ramifications, because other legal instruments, such as laws on data protection, are often constructed around the rights guaranteed by the constitution.

Rights granted under the European Convention[3] relating to freedom of thought and expression are as follows:

- Article 9: Freedom Of Thought, Conscience And Religion -
  - Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, practice and observance.
  - Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others.
- Article 10: Freedom Of Expression
  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. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
  - The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are 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, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Within the UK, because of the lack of any formal rights to privacy or to expression before 2000, the exercise of rights to expression and conscience have often been subject to legal rights in relation to defamation. Other areas of the law (the state censorship laws that existed within the media until the late 1960s, for example, or the recent changes to the law in relation to racial hatred or the expression of support for certain causes considered 'extremist' under the *Terrorism Act 2000*[4]) also consider rights to expression as a negative rather than a positive. The Internet is one area of public policy where, given the mass-media base of the technology, new legislation could reinforce rights to expression in terms of positive rights rather than restrictive penalties. To date, however, because of the emphasis on e-commerce rather than public use of and access to the technology, this has not happened. Nevertheless, there have recently been some efforts at European level to update the framework of fundamental rights[5] in order to reflect technological change.

[2] *European Convention on Human Rights* - http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm
[3] *Human Rights Act 1998* -http://www.legislation.hmso.gov.uk/acts/acts1998/19980042.htm
[4] For more information on the Terrorism Act see the GreenNet briefing no.15 on *New Terrorism Legislation*
[5] See http://europa.eu.int/comm/european_group_ethics/index_en.htm The framework draft itself is available at http://europa.eu.int/comm/european_group_ethics/docs/prodi_en.pdf

The greatest obstacle to the free expression of views (which nevertheless do not offend laws on hate speech or promoting violent or unlawful acts) is the standard contract that users must agree to when signing up for an Internet service. Most standard contracts include conditions relating to defamation. For example Microsoft Network's (MSN's) contract[6] states that users should not,

- Defame, abuse, harass, stalk, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of others. Publish, post, upload, distribute or disseminate any inappropriate, profane, defamatory, infringing, obscene, indecent or unlawful topic, name, material or information.
- Upload files that contain software or other material protected by intellectual property laws (or by rights of privacy of publicity) unless you own or control the rights thereto or have received all necessary consents to do the same.

At the same time, the contract gives the operator the right to limit or discontinue access to the service without requiring evidence that the user has committed an unlawful act, or has actually transmitted material that could be deemed defamatory by a court of law. Again, MSN's standard terms, outlining Microsoft's policy on its control over services, provide a good example here:

- *... Microsoft reserves the right to review materials posted to a Communication Service and to remove any materials in its sole discretion. Microsoft reserves the right to terminate your access to any or all of the Communication Services at any time, without notice, for any reason whatsoever.*
- *Microsoft reserves the right at all times to disclose any information as Microsoft deems necessary to satisfy any applicable law, regulation, legal process or governmental request, or to edit, refuse to post or to remove any information or materials, in whole or in part, in Microsoft's sole discretion.*
- *Termination/Access Restriction: Microsoft reserves the right, in its sole discretion, to terminate your access to any or all MSN Sites/Services and the related services or any portion thereof at any time, without notice.*

The important distinction to be made in these contracts is the difference between the legal basis of an alleged offence, and the ability of a service provider to use their discretion to remove access to services, (and hence limit expression) in the absence of any legally proven case. It is this gap, between legality and discretion, that allows service providers, whether on their own initiative or following pressure from government or industry organisations, to abuse the rights of individuals on the Internet who wish express their views.

The simplest way to balance the individual's rights to expression with the service provider's obligations under the law would be to adopt an external complaints or investigations procedure, or to require that the disconnection of services should only be on the basis of a court order (which the individual would be able to challenge). At the moment, however, pressure within the IT industry to avoid formal regulation means that it is unlikely that any rights of appeal or protection of their rights to expression will be introduced. Service providers' discretionary powers will remain as they stand.

The law of defamation

'Defamation' involves the publication of a statement, reflecting a person's reputation, which tends to lower that person's reputation in the estimation of society. There are two fundamental tests to apply in deciding whether to publish material which may have the potential to defame someone:

- Whether, in terms of the prosecution of a case, the statement made would make an ordinary person in the street modify their opinions of a person as a result of hearing or reading the statement; and

[6]Details of the contract were taken from Microsoft's Hotmail web site - http://www.hotmail.com/

- Whether, in terms of a defence against defamation, the reputation of the 'defamed' person is such that the statement could not conceivably change the average person's views on that person.

Under UK law it is possible to defame corporations as well as individuals.

Defamation can be published in two forms:

- Verbal transmission is classed as slander - and because only the spoken word is involved, slander can often be difficult to prove;
- Written transmission is classed as libel - a case for libel is easier to bring because evidence of the defamation can be documented, and this is the usual form of action taken for defamation.

Given that so much Internet content is made up of the written word, all defamation actions brought in relation to the Internet to date have involved libel. This may change in future, as video and audio streaming become increasingly prominent media. There is, however, no clear legal precedent as to whether the Internet, like other forms of broadcasting, should always be treated as libel, or whether it must in some circumstances be prosecuted as slander.

The other issue with regard to defamation is that the cause of a libel must be 'published'. It is not enough that the words are written just between two friends, or stored on your computer at home, it must be widely 'published'. Therefore you can libel someone using electronic networks by:

- Sending an email, or an email attachment, where that email is widely posted or forwarded;
- Making material available via a web page;
- Posting to an email list or newsgroup; or
- Streaming audio or video via the Net.

Anyone who actively transmits defamatory material is liable as part of any legal action. This, of course, creates problems on the Internet, where many people are involved in the transmission of material. A case for defamation could therefore include not just the author of the material, but anyone involved in the publication or transmission of it; i.e. the owners of the Internet systems forwarding the information, the operators of email lists, web site webmasters, and anyone forwarding the material by email to friends or colleagues.

The Defamation Act 1996[7] is the main law in the UK governing defamation. It outlines the framework for prosecuting cases of alleged defamation, as well as providing various defences for those prosecuted along with the author of the material. To successfully defend against prosecution a person must show that[8]:

- They were not the author, editor or publisher of the material;
- That they had taken 'reasonable care' to prevent the publication of any defamatory material; and
- That they did not know, or had reason to believe, that the material was defamatory, and that their transmission did not contribute to the construction of the defamatory material.

But as part of such a defence, the court will take into account[9]:

- The extent of responsibility the person had for publication (i.e., did they have the ability to prevent publication);
- The nature or means of publication (i.e., whether it was automated, like an email list, or whether the person proactively published the material); and

[7] *The Defamation Act 1996* - http://www.legislation.hmso.gov.uk/acts/acts1996/1996031.htm
[8] Section 1(1) of the Act.
[9] Section 1(5) of the Act.

- How far, by their previous character, the person has a reputation for appropriately testing/vetting the material they publish.

The first major test of the new laws on defamation came with the *Godfrey v Demon Internet* case in 1999. The 1996 Act creates a category of 'special publisher', where the material transmitted is passed automatically by electronic systems without their involvement, or where they are only the suppliers of the equipment or systems that enable publishing or distribution. Demon Internet sought to use this description as part of the case, but lost[10]. This was because Demon Internet carried copies of the newsgroups that contained the defamatory material and, even though they had received complaints about the material, and had the capability to prevent publishing/distribution of the material, they took no action to stop the material being 'published'.

A key difference between broadcasters and Internet service providers is that material that is broadcast only goes out once, unless the broadcaster takes a deliberate decision to keep repeating it. Demon argued that, as the carrier rather than the originator of the material, they were not liable as a 'publisher' under the Defamation Act. The court took a different point of view (hence the settlement of the case out of court). Whilst finding that Demon were indeed not a 'publisher' in terms of section 1 of the Act, the court found them liable because Mr. Godfrey had given them notice that the material was defamatory and they had taken no action to prevent further transmission.

The Godfrey case effectively created *notice-based liability*. If a service provider receives a letter or fax from the offended person stating that the material is defamatory, and subsequently takes no action to restrict the publication of the material, then they become liable. It was for this reason that, in the weeks following the resolution of the Godfrey case, many Internet service providers removed postings and web sites from their servers, even where there had been no complaints against that material[11,] in order to prevent any future claims of defamation against them.

'Notice-based' liability is problematic because:

- Service providers may remove information, or deny access to systems, on the basis of nothing more than a complaint by a person alleging defamation.

This problem may be resolved when a new EC Directive[12] on e-commerce is enacted into UK law. The Directive treats all materials forwarded through email systems as 'traffic'. The Directive discriminates between the roles of the 'originator' of the traffic and the 'carrier', not just in relation to defamation but also in terms of indecency and intellectual property rights infringement. ISPs are not totally exempt however. Under Article 14 of the draft directive an ISP must show they had no knowledge of the 'illegal content'.

Therefore the issue to be settled is whether 'notice liability' exists from the time the offended person first gives notice to the service provider, or whether the offended person must subsequently provide evidence to demonstrate the 'illegal content' before the ISP becomes liable. Given the current legislative timetable it is likely that revisions to the current legal framework will take place as part of new legislation for electronic commerce and electronic media[13], following the recent white paper on broadcasting and the Internet[14].

[10]Note that the case did not proceed to a decision by the court - Demon settled out of court following the payment of £15,000 damages plus costs in March 2000.

[11]The removal of material, particularly material belonging to campaign groups, was widespread, but was particularly prevalent amongst the operators of university web servers.

[12]The draft Electronic Commerce Directive - Com (1999) 427 final - see http://europa.eu.int/ISPO/legal/en/ecommerc/ecommerc.html

[13]For more information on the new electronic media legislation see the GreenNet CSIR Briefing no.11 on *Media and Convergence*

[14]See http://www.communicationswhitepaper.gov.uk/

Defamation actions as a means of silencing criticism

So far we have looked at examples where the Internet service provider of an individual is threatened with legal action. But it is likely that a company or individual may use the threat of a defamation action to silence their critics or campaigners. There have been many examples of this, even before the Internet was a popular communications medium for civil society campaigns[15]. Internet service providers, like other publishers, will not normally defend a claim of defamation. Rather than risk the costs involved in a legal action, many will simply remove the offensive material and undertake not to allow its future publication. But where a claim of defamation is made against the originators of the information or statements they must decide whether to fight the action, because they believe their claims are correct, or to apologise and risk a claim for damages.

The most famous example of such a case, which saw ground-breaking use of the Internet, was the McLibel Trial[16]. In a defamation action by McDonald's against Greenpeace London, two of the defendants used the court case as a campaign opportunity. How the McLibel two took on the McDonald's corporations is a good example of how to handle threats of legal action. Further guidance on how to tackle claims for defamation is also available as part of legal guidelines and case studies produced as part of the GreenNet Internet Rights project[17].

Finally, we have looked so far at situations where a case for defamation is brought following the distribution of material. But there are other options available if those involved have the legal backup. If a person discovers that material that is damaging to their reputation is about to be disclosed, they could bring an injunction to prevent publication (although the injunction would have to be on the basis of the damage it would cause, rather than on grounds of defamation). But if the alleged defamatory material is already in the public domain when the case for defamation is lodged in the court, the persons bringing the action could also request an injunction to force the removal or recall of the material before the case is heard.

Either way, injunctions are a problem; they are an instrument of the court, and therefore if they are ignored or broken they can be instantly actioned and prosecuted, regardless of whether they are justifiable. Given this, and the difficulty of fighting actions through the higher courts, some corporations have recently pursued injunctions rather than prosecutions as a means to tackle problems with groups or campaigns.

The developing law on privacy

There is currently no absolute right to privacy in the UK. However, Article 8 of the European Convention on Human Rights provides that:

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

As the Human Rights Act only came into force in October 2000, the impact of the right to privacy is still not

[15] A good account of corporate legal action against campaigners is contained in Andrew Rowell's book *Green Backlash* - see reference 1 above.
[16] McSpotlight - http://www.mcspotlight.org/
[17] For a index of information available as part of the project see http://www.gn.apc.org/action/csir/

fully tested in the courts. *Douglas & Others* v *Hello! Ltd* (The Times, 16.01.01) was the first several expected cases involving a celebrity and a national publication to come to trial. There have been a number of recent cases where newspapers have published pictures of celebrities in their homes, or other private locations. This has resulted in a number of celebrities threatening to bring actions (at the time of writing) under the right to privacy.

In terms of the Internet and computer networks, rights to privacy are also likely to be involved where personal information is obtained and abused via the Internet. Currently, personal information held by registered data users is protected under the *Data Protection Act*[18]. But there are 'grey areas' where personal information has been obtained from sources other than the person concerned (through photographs, for example. Action under the right to privacy may be possible in these cases if the material compromises a person's privacy, especially if it compromises the person's security or well-being. Whilst action could be brought retrospectively for an invasion of privacy, it is also possible that an injunction could be sought under the right to privacy to prevent disclosure. This is a developing area and it remains to be seen just how the courts will interpret the law here.

Controlling access to material on the Internet

So far we have looked at legal action as the main means of restricting expression. However, technical systems that can be used in computers or Internet servers provide a much simpler, and more effective, means for controlling access to material. There are two main types of system currently available[19]:

- *Filtering* - sifting the packets of data or messages as they move across computer networks and eliminating those containing 'undesirable' material; and
- *Blocking* - preventing access to whole areas of the Internet based upon the address or location.

Filtering operates on the basis of 'rules' that target certain words, phrases or colour combinations in pictures. When the conditions of a rule are satisfied some type of action is triggered. The rules are usually applied as part of the computer program accessing the information, either at the 'socket' where the computer accesses the network, or at the server that routes the information across the Internet. This type of filtering tends to be very crude, because the rules operate without taking account of the context in which the offending term is being used; what is often offensive in one context may be perfectly acceptable in another. Therefore many filtering programs, which are often used in public libraries, schools and other public terminals, can obstruct requests for completely inoffensive material.

Blocking operates in a similar way, but rather than relying on specific rules, the blocking software contains a database of 'restricted' web addresses or email servers. When an attempt is made to access one of the blocked sites the request is refused by the web browser, or the packets or messages are blocked at the network socket or server. A request will also be denied if material is requested from a blocked site as part of an allowed web page.

There are key technical differences in how rules for filtering or lists of blocked sites are determined:

- Rules based systems (filters) - can usually be manipulated by the user, who can make choices as to which words or conditions to filter and can turn filters off or on. But
- Blocking systems - do not allow the user control over the content of the database itself (although addresses may be added to the database.

[18] See the GreenNet CSIR Briefing no.2 on *Data Protection*

[19] There is an excellent database of resources on filtering and blocking software maintained by the Electronic Frontier Foundation - http://www.eff.org/pub/Net_info/Tools/Ratings_filters_labelling/

The database of a blocking system is usually encrypted to prevent access to its contents; this makes it an 'intellectual construct' under intellectual property law[20], and any attempt to decrypt its content, in order to obtain a list of sites being blocked, can result in prosecution by the creators of the software involved.

Concerns have been raised about the use of blocking and filtering software and the impact on freedom of expression. In the US, where blocking and filtering systems are widely used, investigators have found that a wide range of sites are blocked, not merely those deemed 'offensive' because of their sexual or violent content[21]. Increasingly sites are blocked on the basis of their political content. Some studies have found that whilst certain 'offensive' hate sites are blocked, sites (including some belonging to religious groups) which contain other forms of hate speech are not blocked.

Filtering and blocking mechanisms are increasingly being used to control public access to sites critical of the state or the status quo. In some states, for example China and Singapore, 'approved' blocking software must be installed on certain Internet-connected computers. An increasing number of states are beginning to require the installation of this software. In effect, blocking and filtering software becomes a form of 'indirect' state censorship. But because the lists of blocked sites are legally protected under intellectual property rules, it is difficult to have a debate about the civil liberties implications of such censorship.

Further work

This briefing has been written in the context of the legal framework currently in force in the UK. If you live outside the UK you will need to make yourself aware of the procedures operating in your own country. Key points you will need to find out are:

- Does your state provide legal protection for personal privacy, and if so, how does it operate?
- How does your state address the issue of defamation?
- What are the procedures for defining what constitutes defamation, and how are cases brought to court?
- What rights to expression are guaranteed under your state's legal framework? Does it include any special protection against defamation - for example for teachers, journalists or researchers?
- What are the current requirements for the fitting of filtering or blocking software in your country? Are these general requirements or is there an approved list of systems that must be used?

You should also contact any civil liberties organisations operating in your country. They may be able to provide you with much of the information you need on laws relating to freedom of expression, defamation and privacy.

The GreenNet Internet Rights Project

GreenNet[22] is the UK member of the Association for Progressive Communications[23] (APC), and is leading

[20] See CSIR Toolkit Briefing no. 7, *Intellectual Property*
[21] See the EPIC report, *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet* - http://www.epic.org/reports/filter-report.html
[22] GreenNet - http://www.gn.apc.org/
[23] APC - http://www.apc.org/

the European section of the APC's Civil Society Internet Rights Project[24]. The primary goal of this project is to provide the resources and tools necessary to defend and expand space and opportunities for social campaigning work on the Internet against the emerging threats to civil society's use of the 'Net. This involves developing ways and means of defending threatened material and campaigning, as well as lobbying to ensure a favourable legal situation for free expression on issues of public interest.

Until recently, the social norms of Internet communities, together with a very open architecture based on supporting these norms, regulated the Internet, and was responsible for its openness. The main forces of regulation now, however, are the business sector and government legislation. Corporations and governments are pressing for fundamental changes in legislation and in the architecture of the Internet. Unless challenged, these moves could radically change the nature of the 'Net, making it a place of oppressive controls instead of freedom and openness. It is in this context that APC's Internet Rights project is being developed.

This briefing is one in a series[25] that document different aspects of work and communication across the Internet. Although written from the perspective of the UK, much of its content is applicable to other parts of Europe. There is continuing work on these issues, as part of the European project. If you wish to know more about these briefings, or the European section of the APC Civil Society Internet Rights Project, you should contact GreenNet. You should also check the APC's web site to see if there is already a national APC member in your country who may be able to provide local help, or with whom you may be able to work to develop Internet rights resources for your own country.

Free Documentation License:

For more information about the Civil Society Internet Rights Project, or if you have questions about the briefings, contact ir@gn.apc.org.

[24] CSIR Project - http://rights.apc.org/
[25] http://www.internetrights.org.uk/