Parliamentary Office of Science and Technology

postnote

June 2001 Number 159

REGULATING INTERNET CONTENT

Concerns over the nature of some publicly available material on the internet have led to calls for stricter regulation. Opponents point to the technical and legal difficulties of regulation in a global and unlicensed environment, as well as disquiet over restraining trade and personal liberty. The recent Communications White Paper included no plans to introduce statutory internet content regulation, but the remit of the new communications regulator (Ofcom) would cover internet content. This note considers options for regulation and examines Government policy in this area.

What is the internet?

The internet links computers worldwide, enabling a person at one computer to interact with other computers. There are a number of terms to describe such a system, including *online* and *cyberspace*. Individuals gain access to the internet through an Internet Service Provider (ISP). In the UK, 35% of homes have internet access, and 51% of adults have used the internet. The internet includes:

- email: sending messages from one person to another electronically.
- the world wide web (www): allows any computer to publish documents annotated with links to other material (which may be on a different computer). Web pages can include other internet applications, such as music and video.
- usenet: electronic bulletin boards, containing tens of thousands of 'newsgroups' about specific subjects.
- chat: real time text or voice conversations between users in an online 'chat room'.

Creating internet content

Unlike traditional broadcast media, internet content can be 'published' by anyone with a computer and internet access. Sending email or submitting information to news groups requires little technical knowledge. There are also web sites which help users create their own web pages, and ISPs may 'host' these for individuals. This liberated environment has been one of the reasons for the internet's rapid growth, enabling anyone, from school children to multinational businesses, to publish their own web pages which are then available worldwide. There are estimated to be over 2 billion publicly accessible web pages, although the most-accessed web sites are dominated by large companies.

Why regulate?

The wide range of material on the internet inevitably means that some illegal content is obtainable, such as child pornography, breaches of copyright, financial frauds, etc. Other universally available content is considered unacceptable by certain people for social, political and moral reasons - for example, adult pornography, racial abuse and political criticism. Estimates of the amount of objectionable material on the internet vary greatly, but research suggests that about 3% of web pages contain sexually provocative material and 0.7% have notable violent content[1]. Easy availability of such material has led to pressure for regulation.

However, opinions differ as to how - and indeed whether - the internet should be regulated. At one end of the spectrum are countries such as Saudi Arabia and China that have attempted to control citizens' access to the internet to suppress the dissemination of dissident ideas. In contrast are those who argue that regulating the internet would be undesirable because its open and unregulated nature, along with very low entry costs, has encouraged commercial and social innovation and self-expression. There are also concerns that regulation could jeopardise legitimate trade and national competitiveness.

Regulatory options

Because the internet is a global medium with no central control, it is impossible to monitor and remove objectionable content completely. However, it is possible to make it more difficult to access, and for barriers to be placed in the way of businesses providing such content. There are three main types of regulation:

- **Statutory regulation**. The internet is international and providing content does not require a licence, so such traditional mechanisms are difficult. Illegal content may be removed using basic law and international agreements, but failure to enforce by any country globally can result in continued universal availability.
- **Self-regulation by industry**. Because of a desire to avoid statutory regulation and the legal difficulties of enforcement, this is often the preferred option – for example, the Internet Service Providers Association Code of Practice (www.ispa.org.uk). Where Government plays a more active role, this is known as co-regulation. However, self-regulation can lead to market openings for service providers who bypass such standards.
- **Individual regulation.** By using filtering software, individuals can at least partially block access to content (see box opposite). This avoids restricting the content at source, and can allow the user to set their own standards. But such software is not a substitute for parental supervision of children's internet use – filters are not always reliable and vary in the control they allow - and requires user education. Media literacy can also help users avoid objectionable content – for example, by knowing which web sites are likely to be suitable.

Government proposals - Ofcom

The December 2000 White Paper *A New Future for Communications* proposed the creation of a single communications regulator, Ofcom, merging 5 regulators:

- Oftel, which regulates telecommunications services.
- Independent Television Commission (ITC), which licenses and regulates commercial television services.
- Broadcasting Standards Commission, which regulates standards and fairness in broadcasting.
- Radiocommunications Agency, which has responsibility for managing the radio spectrum
- Radio Authority, which licenses and regulates all commercial radio services.

A draft Bill was announced in the Queen's speech for 2001/02, and the Government aims to bring Ofcom into operation by 2003. Under these proposals, Ofcom would regulate traditional broadcast content via a three tier structure, with tier one applying to all broadcasters and tiers two and three those with a public service remit. Internet content would remain outside this structure, in 'tier zero'. These proposals are discussed on page 4.

Issues

Illegal content

Laws apply online in the same way as they do offline, but the international nature of the internet takes much of such content outside national jurisdiction. Although this makes policing content difficult, it also makes the internet a powerful tool for freedom of speech, enabling the publication of critical commentary in countries with restrictive regimes. A distinction thus needs to be drawn between that which is widely illegal (for example, child pornography) and that which is culturally specific (such as adult pornography or political commentary).

Types of filtering and rating

Filters that use a pre-selected list of sites. Lists of objectionable sites are provided by the filtering company and access to these sites is blocked. Alternatively, lists of recommended sites can also be provided ('Yes lists'), but can be very restrictive as access to many innocuous sites not on the list is blocked. Such lists can be compiled by hand or automatically and must be updated regularly.

Keyword based filters. These search web sites for a list of objectionable keywords, such as sexually explicit terms or racial abuse. They then block sites where keywords are found. Early versions of such filters were very crude, but increasing use of artificial intelligence techniques allows some to analyse the content of a site, so that innocuous content (for example, 'breast cancer') is not blocked.

Ratings based filters. A coded label is placed on each web site, which describes its content. Internet users then set their browser to accept or reject sites with (or without) certain labels. The labels can be set by the content provider, or by independent groups, and people can choose which labelling body they use. There are international bodies which set standards for such ratings, for example the Internet Content Rating Association (www.icra.org).

Blocking outgoing information. These tools allow parents to control what information children send to the internet. For example, addresses and telephone details could be withheld.

Positive content. Many web sites are aimed at children, or contain links to direct children towards appropriate material. Some internet search engines allow parents to configure them to return only unobjectionable content in search results, although they do not block access to other sites. Another approach is to allow access only to a pre-selected section of web sites ('walled gardens').

Monitoring. Programmes are available which will run in the background on a computer, recording all online activity or attempts to view certain sites. Rather than blocking access to web pages, such tools can be used as a deterrent.

Sources: www.getnetwise.org/tools/proscons.shtml
www.research.att.com/~lorrie/pubs/tech4kids/actions.html

In the UK, the Internet Watch Foundation (IWF, www.iwf.org.uk) addresses illegal material on the internet, particularly child pornography. Funded by the internet industry and the EU, the IWF runs a hotline for users to report potentially illegal content. After assessing the report, the IWF trace the computer (server) hosting potentially illegal material. For UK-based servers, the IWF pass this information to the National Criminal Intelligence Service, who forward details to the relevant police force or overseas authorities. A UK ISP holding such content is also advised and faces prosecution if it does not remove the material.

Since its inception, the IWF has been instrumental in the removal of 28,000 images of child pornography from UK servers (although these images may remain accessible to UK residents on overseas servers). A number of other countries also host similar hotlines (www.inhope.org). In the Communications White Paper, the Government expressed continued support for the IWF, whose remit is expanding to cover racially offensive material. However, the IWF is not a public body, and extension of its role could raise questions over accountability.

Another internet content regulator is ICSTIS, which is responsible for internet services provided over premium rate telephone lines. In April 2001, the Government launched the National High Tech Crime Unit, to investigate serious and organised crime on the internet. Of the £25m funding allocated over 3 years, £10m will be used to develop local computer crime units. It is not within the scope of this note to consider wider illegal internet content issues such as cybercrime, fraud, privacy and junk email[2]. However, some specific e-commerce issues are discussed in the box below.

E-commerce and consumers

Much use of the internet for commerce is already covered by existing regulators. For example, online banking is regulated by the Financial Services Authority and data protection by the Office of the Information Commissioner. Similarly, goods purchased online are covered by trading standards, advertising by the Advertising Standards Authority, etc. But because of its global nature, e-commerce raises issues of jurisdiction. The E-commerce Directive sets down the principle that e-traders are bound by the law in the country where they are established. However, under other EU regulations, consumers can sue in the country where they live if the supplier has 'directed his activities' towards the consumer's member state. Law in this area is very complex, both for consumers and traders, and many concerns have yet to be resolved.

Consumer protection laws are also set out in the EU's Distance Selling Directive. Many online traders do not yet comply with these new regulations: trading standards officers who surveyed 102 UK-based sites had a range of problems with their orders, affecting more than one third of cases. One self-regulatory attempt to address the issue of consumer confidence is TrustUK, which is endorsed by the Government. It accredits existing industry codes of practice, whose members can then display the TrustUK logo. However, the issue of consumer 'kite' marks is currently under review, both in the UK and Europe.

Concerns have been expressed over the resources and training available to trading standards officers, and how international co-operation to enforce standards can be encouraged. In their June 2001 report, '*Surfing the Big Wave*', the Trading Standards Institute made extensive recommendations for improving Trading Standards professionals' knowledge of e-business, in order to boost consumer confidence online (www.tradingstandards.gov.uk).

Liability of service providers

Last year, a French judge ruled that French internet shoppers should be barred from accessing *Yahoo!* auction sites selling Nazi memorabilia. The sale of items which incite racial hatred is illegal in France. Although *Yahoo! France* web sites did not sell such material, *Yahoo!* sites in the US did. It would be impossible to block all French users from accessing such sites, but the court heard evidence that it would be feasible to block the 70% of surfers who use an easily identifiable French ISP. In fact, other internet retailers and auction sites employ similar methods, such as software which examines delivery addresses for goods, although these are by no means infallible. *Yahoo!* is currently contesting the validity of the ruling in a US court. The decision raises questions over jurisdiction and service providers' legal duties in all countries where they have a presence. International agreement would be required to ensure compliance with any ruling in an overseas court.

Material held on web sites can contravene a wide range of laws, such as illegal use of trademarks or copyright. Under the EU Electronic Commerce Directive, which must be translated into UK law by January 2002, an ISP is not liable for information it transmits (it is a 'mere conduit'). In 1999, *Demon Internet* in the UK paid damages for failing to remove a defamatory posting on a newsgroup carried on its servers. Because *Demon* had been informed of the defamatory content, the judge ruled that the ISP was responsible for the postings. However, critics have noted[3] that such laws encourage ISPs to remove any potentially illegal content whenever it is notified to them, effectively casting the ISP in the roles of defendant, judge and jury.

Chat rooms

Internet chat rooms aimed at children can attract paedophiles who may attempt to arrange meetings with young users. This often involves introducing sexual themes into conversations and attempting to persuade them that such behaviour is appropriate (known as 'grooming'). Organisations such as Childnet International (www.childnet-int.org) have suggested a range of measures, including warning messages in children's chat rooms. They also suggest examination of whether the law should be changed to make it easier for police to pose as children in chat rooms and hence identify and charge paedophiles (this is already permitted in the USA).

In response to the Internet Crime Forum's March 2001 *Chat Wise Street Wise* report[4], the Home Office has set up a task force involving representatives of the internet industry, child welfare organisations, the police and Government. It will consider chat rooms, availability of child pornography on the internet, partnerships between ISPs and the police, and increasing parental confidence. The task force's next meeting, in summer 2001, will examine possibilities for a new law to prevent online grooming. Companies that run chat rooms have also come under pressure - *Yahoo! UK* has appointed an adviser whose remit includes improving child safety online. Some children's chat rooms have a trained adult host present, to monitor content.

Rating and filtering

As discussed previously, filtering software is not failsafe - it can block access to potentially valuable web sites

(such as www.parliament.uk, which does not have a rating label) while allowing objectionable content. Such software also varies in the extent to which users can customise the filters. Further, third party rating raises issues of transparency and the imposition of moral values by unaccountable bodies. It is also possible for service providers (or Governments) to include filters without the user's knowledge, restricting individual choice and access to information – although technical solutions allow filters to be bypassed, for example by encrypting the web page.

The Government has expressed its support for rating and filtering, and the Home Office recently labelled its web site. Research by the European Commission is examining ways to improve such services. However, these schemes depend on widespread adoption of international standards. In addition, if they are to employ these tools, users must be aware of their advantages and disadvantages. One of Ofcom's roles would be to promote media literacy, working with industry and educators. This could include increasing awareness of rating and filtering.

Intellectual property

The internet allows copyright laws to be broken easily. Material can be copied and distributed widely without the need for specialist equipment. Programmes such as *Napster* and *Gnutella* have shown how the internet can enable users to search each other's computers for music files on a large scale (at its peak, *Napster* had over 80 million registered users). This is known as peer-to-peer file sharing. Legal action has forced *Napster* to redefine its business model, levying a monthly charge for services and forming alliances with record companies. But other file sharing programmes do not rely on a central server, and so are less vulnerable to law enforcement. At present, concerns focus on music because these files are small enough to download in a few minutes. Once users have faster internet access, films, TV programmes and computer games could also be shared in similar ways.

Technical solutions are available, such as digital 'watermarks' which allow illegally copied music to be identified. However, incorporating inaudible watermarks in music is difficult and software solutions may be cracked by programmers. The recently approved EU Copyright Directive attempts to protect copyright holders while permitting private copying of audio and video material. It allows for 'technological measures', such as encryption, to prevent unauthorised copying, and makes it illegal to circumvent these measures.

Broadcast content

The Communications White Paper proposes that no statutory regulation by Ofcom be applied to the internet. This has been widely welcomed. However, some have expressed concern over the possibility of 'regulatory creep'. For example, the White Paper expects public service broadcasters to apply the same standards online as offline – such as in supplying impartial news. Ministers stressed in evidence to the House of Commons Culture Media and Sport Select Committee that the White Paper did not intend new proposals for internet regulation. To clarify this, the Committee recommended that Ofcom be "*excluded by statute from imposing regulatory obligations relating to internet content*", including on public service broadcasters.[5] The Government has an opportunity to make its position clear in its reply to the Select Committee, which is expected before the summer.

It is envisaged that the regulatory structure established by the Bill would last for ten years, but legislating for the swiftly changing communications market is difficult. With faster internet connections, much licensed television content could also be available on the internet[6]. This may raise fundamental questions for broadcast regulation. The ITC points out that at present citizens have different expectations of TV and internet regulation. A key current distinction is that between content 'pushed' into the home (such as broadcast television), and 'pulled' content (for example, selecting a web site). Under Ofcom, tier one regulation setting universal negative content standards would apply to 'pushed' services, where viewers are seen as having less choice over what they receive.

With a much wider range of channels and interactive services, delivered over the internet or via digital TV, it is conceivable that this distinction could become untenable. On this subject, the Select Committee concluded that in future universal negative content regulation would cease to be possible. However, they saw a case for continued positive programming requirements on broadcasters in receipt of direct or indirect public service subsidy.

One of Ofcom's duties will be to promote media literacy, helping people understand diverse media services and the differences between them. The White Paper recognises that the wider availability of material, for example on the internet, will necessitate people taking more individual responsibility for their own and their family's media use. But it still sees a role for industry in developing tools to aid navigation and control of communications media.

Endnotes

1 *Risk and the Internet: Perception and Reality*, E. A. Zimmer and C. D. Hunter, University of Pennsylvania
2 See POST report 114, April 1998, *Internet Commerce: threats and opportunities* for discussion of wider internet issues
3 e.g. Yaman Akdeniz, director of Cyber-Rights & Cyber-Liberties (UK)
4 *Chat Wise, Street Wise – children and Internet chat services:* www.internetcrimeforum.org.uk. The Internet Crime Forum brings together government, law enforcement agencies and industry.
5 *The Communications White Paper*, Second Report of the Culture Media and Sport Select Committee, March 2001
6 See forthcoming POST report on convergence of digital media.

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of public policy issues that have a basis in science and technology.

The Parliamentary Office of Science and Technology, 7 Millbank, London SW1P 3JA Tel 020 7219 2840

www.parliament.uk/post/home.htm