# Internet regulation

Standard Note: SN06145
Last updated: 1 December 2011
Author: Grahame Danby
Section Science and Environment

The practicalities of blocking and filtering harmful material on the internet have generated interest in a range of contexts: the misuse of social media during the August 2011 riots, child sexual abuse images and copyright infringement.

The communications regulator, Ofcom, considered a range of blocking techniques in the context of combating copyright infringement. Ofcom reported in May 2011. In August 2011, the Department for Culture, Media and Sport published *Next steps for implementation of the Digital Economy Act*. This referred to Ofcom's assessment of website blocking and the fact that the Government would not be proceeding with this for the time being.

Other legislation can also be invoked to control internet content. Section 127 of the *Communications Act 2003* proscribes the improper use of a public electronic communications network. It has recently been applied, apparently for the first time, to a social networking site (Twitter).

Online activity is also subject to general offline legislation such as the *Obscene Publications Act 1959* and the *Human Rights Act 1998*.

Tackling internet hate crime is another area that poses a challenge to the adaptation of law to this medium. A new service for reporting all hate crimes online was launched by the police in April 2011.

## Contents


| | | |
|---|---|---|
| **1** | **Website blocking** | **2** |
| **2** | **Digital Economy Act** | **3** |
| **3** | **Communications Act** | **3** |
| **4** | **Obscene Publications Act** | **4** |
| **5** | **Human Rights Act** | **5** |
| **6** | **Internet hate crime** | **7** |


## 1 Website blocking

Access to harmful content can be stopped in a number of ways. Most internet service providers (ISPs) block access (by anyone) to websites known to contain images of child sexual abuse ("child pornography"). The Internet Watch Foundation (IWF) maintains a list of offending websites which is updated twice daily. The list typically contains details of 500 websites. The IWF considers this kind of blocking to be "a short-term disruption tactic which can help protect internet users from stumbling across these images, whilst processes to have them removed are instigated." It is highly unlikely to be a suitable approach for adult pornography or violent material much of which is legal (at least if it is unavailable to minors)[1] and which is prevalent on the internet. However, this kind of blocking (known as uniform resource locator blocking) is only one of a number of available techniques.

The communications regulator, Ofcom, considered a range of blocking techniques – albeit in a different context – in its report of May 2011, *"Site Blocking" to reduce online copyright infringement*. The techniques considered were termed "primary" on account of their allowing ISPs to apply blocking at the level of their network infrastructure. Although none of the specific techniques are failsafe, they aim to prevent harmful material reaching any device within the home. The main alternative currently used is to install software on individual devices in the home to block the display of material identified as being harmful. One problem with filtering and blocking techniques is that legitimate websites can sometimes be captured. Deliberate circumvention by IT-literate users is also a challenge.

The ISP, TalkTalk, offers "opt-in network level filtering". The large ISPs have been working on developing a code of conduct on child protection. An online article in *eWeek Europe* (12 October 2011) outlined the current position:

> Virgin Media, BT, Sky and TalkTalk have discounted suggestions that their new child-protection measures will oblige users to "opt in" in order to view material deemed inappropriate for children.
>
> The four ISPs said yesterday they would begin offering customers an "active choice" at the point of purchase to block adult content. This has led to suggestions that a new "filtered feed" will be applied to everyone using Internet connections provided by the ISPs – including existing customers – requiring them to actively opt in to view this material.

---

[1] The test of obscenity under the *Obscene Publications Act 1959* takes into account the effect on the viewer of the material in question.

> However, the ISPs have clarified that existing customers will see "absolutely no difference" to their web content. The new measures brought in by the ISPs chiefly amount to a new voluntary code of practice that will include the principle that users should be asked whether they want to activate parental controls when they buy a new contract.
>
> [...]
>
> Virgin Media, BT and Sky will offer the child protection features via PC-based software offered on the customer's installation disk, while TalkTalk is offering network-based content filtering.[2]

## 2 Digital Economy Act

Sections 17 and 18 of the *Digital Economy Act 2010* cover website blocking, albeit in connection with copyright infringement:

- "Power to make provision about injunctions preventing access to locations on the internet"
- "Consultation and Parliamentary scrutiny"

In brief the effect of these sections is to introduce a power to bring in regulations for website blocking – subject to a "superaffirmative" parliamentary procedure.

The Secretary of State could make the relevant regulations – but only a court could order the blocking of a website once (if ever) such regulations provide for this.

In August 2011, the Department for Culture, Media and Sport published *Next steps for implementation of the Digital Economy Act*. This referred to Ofcom's assessment of website blocking and the fact that the Government would not be proceeding with this for the time being:

> The DEA contains reserve powers to tackle copyright infringing websites through a court based process to block access to these sites. Following concerns raised in the Your Freedom exercise last year, the Government commissioned Ofcom to report on the practical workability of these measures. We are publishing that report today. Ofcom concludes that the blocking of infringing sites could potentially play a role in tackling online copyright infringement, but that the approach set out in the DEA is unlikely to be effective because of the slow speed that would be expected from a full court process. This would provide site operators with the opportunity to change the location of the site long before any injunction could come into force.
>
> The Government will not bring forward regulations on site blocking under the DEA, at this time. However, we are keen to explore the issues raised by Ofcom's report and will be doing more work on what measures can be pursued to tackle online copyright infringement.

## 3 Communications Act

Section 127 of the *Communications Act 2003* proscribes the improper use of a public electronic communications network. It has recently been applied, apparently for the first time, to a social networking site (involving a reference on Twitter to bombing an airport). Background to this case (currently subject to appeal) involving Paul Chambers is widely

---

[2] "ISPs Defend New Porn Filtering Measures", *eWeek Europe*, 12 October 2011

available online.[3] It is worth commenting that the application and interpretation of the relevant statute law as it applies to the internet is still at a relatively early stage of development.

Section 127 of the Act is reproduced below:

> 127 Improper use of public electronic communications network
>
> (1) A person is guilty of an offence if he—
>
> (a) sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or
>
> (b) causes any such message or matter to be so sent.
>
> (2) A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he—
>
> (a) sends by means of a public electronic communications network, a message that he knows to be false,
>
> (b) causes such a message to be sent; or
>
> (c) persistently makes use of a public electronic communications network.
>
> (3) A person guilty of an offence under this section shall be liable, on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale, or to both.
>
> (4) Subsections (1) and (2) do not apply to anything done in the course of providing a programme service (within the meaning of the Broadcasting Act 1990 (c 42)).

## 4 Obscene Publications Act

While the *Obscene Publications Act 1959* tends to focus on sexual material, it could in principle also apply to violence in a non-sexual context.[4]

Publication of obscene material, including child pornography and extreme adult pornography, is illegal under the *Obscene Publications Act 1959* (which extends to England and Wales). Section 2 (as amended by the *Obscene Publications Act 1964*) prohibits the "publication" of obscene material. Subsection 1 reads:

> (1) Subject as hereinafter provided, any person who, whether for gain or not publishes an obscene article or who has an obscene article for publication for gain (whether gain to himself or gain to another) shall be liable—
>
> (a) on summary conviction to a fine not exceeding the prescribed sum or to imprisonment for a term not exceeding six months;
>
> (b) on conviction on indictment to a fine or to imprisonment for a term not exceeding three years or both.

---

3 "Twitter airport 'joke' trial heads to the High Court", *BBC News*, 22 November 2010

4 Geoffrey Robertson QC and Andrew Nicol QC, *Media Law*, 5th edition, 2007, p216

For the purposes of the Act publication includes the distribution, circulation, sale, giving or loan of the obscene article.[5] An important point is that the definition of obscene depends partly on the person who sees the material. Thus, section 1 of the Act begins:

> (1) For the purposes of this Act an article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.
>
> (2) In this Act "article" means any description of article containing or embodying matter to be read or looked at or both, any sound record, and any film or other record of a picture or pictures.

The following passage in Tom Crone's book, *Law and the Media*, provides an illustration:

> The 1959 Act modifies the common law test [of obscenity] set out in *R v Hicklin*. It changes the type of person likely to be depraved from those into whose hands it 'may fall' to those to whom the material is likely to be given or sold. For example, 'adult' material sold in a sex shop will not be obscene under the 1959 Act just because its effect would be to 'tend to deprave' a child, because in normal circumstances this sort of adult material will not be sold to children. On the other hand, adult material published in a national newspaper that is available and likely to be read by almost every section of the community, including children, is likely to be obscene.[6]

## 5 Human Rights Act

If feasible, preventing access to online media by individuals wishing to organise violent disorder would be unlikely to infringe their human rights. In the UK the relevant legislation is the *Human Rights Act 1998* which gives further legal effect to the fundamental rights and freedoms contained in the European Convention on Human Rights. The right to free speech, for example, is a qualified right. Article 10 of the European Convention on Human Rights embodies this right as well as circumscribing it:

> Article 10 – freedom of expression
>
> 1. 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.
>
> 2. 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.

---

5 *Obscene Publications Act 1959*, section 1(3)

6 Tom Crone, *Law and the Media*, fourth edition, p206

Unsurprisingly, the misuse of Facebook, for example, to incite violence is a breach of that website's terms of use. These largely comprise a *Statement of Rights and Responsibilities* from which the following extracts are taken:

> By using or accessing Facebook, you agree to this Statement.
>
> [...]
>
> We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to do that, which includes the following commitments:
>
> [...]
>
> You will not post content that: is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
>
> [...]
>
> You will not facilitate or encourage any violations of this Statement.
>
> [...]
>
> We respect other people's rights, and expect you to do the same.
>
> You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
>
> We can remove any content or information you post on Facebook if we believe that it violates this Statement.
>
> [...]
>
> If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account.

It seems unlikely that social media sites could respond with sufficient speed to a rapidly evolving situation of the kind associated with the recent riots in English cities – which is not to say that there is no scope for some action on their part.

A Westminster eForum Keynote Seminar, *eCrime, cyber-threats and protecting critical infrastructure* took place in London on 24 November 2011. At least one speaker referred to social media as "open source intelligence". It can help police track down perpetrators and in cases prevent disorder. When someone in Manchester tweeted that they would be starting a riot in a certain area, the police tweeted back words to the effect of "We'll see you there". This approach of engaging with social media was viewed, again by some speakers, as being more intelligent than the deployment of blunt instruments like disconnection. The Government's suggestion that social media sites might be disconnected to deal with disorder was, apparently, also met with interest by some countries not known for their commitment to human rights.

Speaking at the London Conference on Cyberspace (1-2 November 2011), the Foreign Secretary (William Hague) said:

> Earlier this year I proposed the following principles for governing behaviour in cyberspace, and called for a more focussed and inclusive dialogue between all those

with a stake in the Internet – civil society and industry as well as governments - on how we might implement them:

1. The need for governments to act proportionately in cyberspace and in accordance with national and international law;

2. The need for everyone to have the ability – in terms of skills, technology, confidence and opportunity – to access cyberspace;

3. The need for users of cyberspace to show tolerance and respect for diversity of language, culture and ideas;

4. Ensuring that cyberspace remains open to innovation and the free flow of ideas, information and expression;

5. The need to respect individual rights of privacy and to provide proper protection to intellectual property;

6. The need for us all to work collectively to tackle the threat from criminals acting online; and

7. The promotion of a competitive environment which ensures a fair return on investment in network, services and content.

## 6 Internet hate crime

A new service for reporting all hate crimes online was launched by the police in April 2011. The website, called True Vision, is supported by all forces in England, Wales and Northern Ireland and can be accessed at www.report-it.org.uk. All reports of incitement to racial hatred content hosted in the UK previously reported to the Internet Watch Foundation (IWF) should now be reported directly to True Vision. The True Vision website includes an overview of what can be done about hate crime on the internet:

> While you may come across a lot of material on the internet that offends you, very little of it is actually illegal. UK laws are written to make sure that people can speak and write, even offensive material, without being prosecuted for their views. Parliament has tried to define laws in a way that balances our freedom of expression with the right to be free from hate crime.
>
> Agencies like the police have duties to promote good relationships between different parts of our communities, but they do not have powers to control offensive thoughts or words unless they are shared illegally. We understand that hate material can damage community cohesion and create fear, so the police want to work alongside communities and the Internet industry to reduce the harm caused by hate on the Internet.
>
> […]
>
> In England and Wales it can be an offence to stir up hatred on the grounds of:
>
> - Race
> - Religion
> - Sexual Orientation.
>
> (There is no similar offence relating to disability or transgender)

[…]

The content of a website can also be illegal when it threatens or harasses a person or a group of people. If this is posted because of hostility based on race, religion, sexual orientation, disability or transgender then we consider it to be a hate crime.

Illegal material could be in words, pictures, videos, and even music and could include:

- messages calling for racial or religious violence
- web pages with pictures, videos or descriptions that glorify violence against anyone due to their race, religion, disability, sexual orientation or because they are transgender.
- chat forums where people ask other people to commit hate crimes

[…]

*Websites from outside the United Kingdom*

The Supreme Court has indicated that an offence is committed where the person posts or controls the material in this country. Therefore, much material that can be viewed in the UK is outside the jurisdiction of our courts. The USA, for instance does not have offences of inciting racial hatred but if someone inside the UK posts on a foreign site then that could still be illegal here. (The person posting is always responsible for their content and web hosts could be if they, for instance, encourage or knowingly allow it to remain)

*What you can do about online hate material*

Most hateful or violent website content is not illegal but you can still take the steps below to have it removed if it upsets, scares or offends you.

*Option One - Report it to the website administrator*

Most websites have rules known as ‘acceptable use policies’ that set out what cannot be put on their website. Most do not allow comments, videos and photos that offend or hurt people.

Popular websites such as Facebook, YouTube or BBC News have simple ways for you to complain about a page or video.

If what you’ve seen is on a site with a good complaints system, you should report it to the website’s owners. Look out for their ‘contact us’ page, which should be clearly linked.

Others will have a ‘report this page’ button that you can click.

*Option Two - Report it to the hosting company*

If the website itself is hateful or supports violence then let the website’s hosting company know.

Hosting companies provide a place where the website sits, and often have rules about what they are willing to host. Let the hosting company know they are hosting a website that breaks their rules, and ask them to stop.

You can find out which company hosts a website by entering their web address on the 'Who is hosting this?' website.

You can also contact your own internet supplier to get more information.

*Option Three - Report illegal Internet material to the police*

If the website you have seen online matches the description of illegal content above and you think it originates in the UK, you should report it to the police.