Censorship or Common Sense?
Mark Gracey (mark.gracey@thus.net)
THUS plc

Abstract

In 1995 the Internet was in its infancy, email was the killer application and the World Wide Web looked like it had potential. Ten years on and the Internet touches our lives in many ways, some of which are less desirable than others. The Internet was never intended to introduce new forms of crime or to make illegal material more readily available, but this is a reality we must all accept.

Internet Service Providers (ISPs) are addressing these problems in different ways. In 2004 BT introduced a trial web filter which blocked sites hosted outside the UK which are reported by the Internet Watch Foundation as illegal. Some ISPs have opted for a ‘walled garden’ approach in which customers can only access selected material, while others have focused on helping their customers use web-filtering products. Market forces and demand for ISPs services will inevitably drive forward better protection from the dangers we all face online, but how this will be achieved is going to vary.

This paper will look at network-level web blocking technology, whether it works, whether it is practical and what sort of service an ISP’s users will expect it to provide. It will also consider whether filtering in this way puts the ISPs at risk or whether alternative approaches like education and awareness are the key. Comparisons will be drawn from around the world where various regimes exist to deal with unwanted content.

Introduction

When the commercial use of the Internet started in the early 1990s no one would have guessed that it would have the impact on our society that it has today. Or that 52%\(^1\) of the UK population would have direct access to it in their homes. It would seem that there is something on the Internet for everyone. With its diverse set of tools: email, the world wide web, usenet and chat, the Internet is available to most, if not at home then at school or in the work place.

But no one anticipated that it would be adopted and proven so successful for a wide range of illegal activity or for the distribution of such a diverse range of offensive material.

Although in general the Internet is a safe place, where benefits far outweigh the impact of illegal activity, there is no doubt that illegal activity and access to unsuitable material is a

\(^1\) http://www.statistics.gov.uk/CCI/nugget.asp?ID=8&Pos=&ColRank=1&Rank=374
considerable concern for everyone. Fuelled by the media, stories of child abuse images (e.g. Operation Ore\(^2\)), paedophiles meeting children they have met online (e.g. the case of Michael Wheeler\(^3\)), or the increase in spam messages does nothing but raise concern with the general public, politicians and interest groups alike, about the Internet and its use.

ISPs have a role to play in addressing these issues and there are a number of ways in which they do this, be it membership of organisations like the Internet Watch Foundation, working with government through groups like the Home Secretary’s Task Force for the Protection of Children Online, or by implementing child friendly services.

### Protecting the vulnerable

Preventing access to different types of material can be achieved in a number of ways:

- Self or co-regulation
- Legislation
- Education
- Restricting access

Self-regulation requires the industry to provide its own solution to an issue. This may be done via codes of practice, for example, which set out what companies will do or how they will deal with a particular issue. A self-regulatory regime has no statutory backing, no supporting legal framework and no intervention by a government. It is purely an industry’s approach to enforcing its own controls.

Some examples include: The Banking Code\(^4\), the London Internet Exchange’s (LINX’s) Best Current Practice\(^5\), ISPA’s code\(^6\) and service providers’ acceptable use policies (AUPs)\(^7\). These are all examples of where a code has been produced, sometimes in consultation with users or even with governments, but where the sanctions (if relevant) imposed are enforced under their own regimes rather than by legislation.

---

\(^3\) [http://news.bbc.co.uk/1/low/england/cambridgeshire/2969020.stm](http://news.bbc.co.uk/1/low/england/cambridgeshire/2969020.stm)
\(^4\) “The Banking Code sets minimum standards of good service that you can expect from banks, building societies and other providers of banking services.” [http://www.bankingcode.org.uk/pdfdocs/bankcodeflyermarch03.pdf](http://www.bankingcode.org.uk/pdfdocs/bankcodeflyermarch03.pdf)
\(^5\) [http://www.linx.net/noncore/bcp/index.thtml](http://www.linx.net/noncore/bcp/index.thtml)
\(^7\) e.g. [http://www.demon.net/helpdesk/aup/](http://www.demon.net/helpdesk/aup/), [http://www.ja.net/documents/use.html](http://www.ja.net/documents/use.html) and [http://www.freeservers.com/policies/acceptable_use.html](http://www.freeservers.com/policies/acceptable_use.html). All set out guidance for their users on what will not be tolerated on their services.
A co-regulatory approach also uses best practice or industry codes usually put together by the industry, but supported by legislation. For example the Broadcasting Standards Commission (BSC)\(^8\) code was set up under the Broadcasting Act 1986 and membership is compulsory for all UK broadcasters another example is the ICSTIS code\(^9\).

The IWF is a co-regulatory body that deals with the take down of illegal child abuse images. The law makes possession and distribution of such images illegal and the IWF model ensures that any such material hosted in the UK is removed from the Internet. The IWF works based on an agreement put in place between the Internet industry, law enforcement agencies and government and supported by certain pieces of legislation\(^10\).

The UK government favours a self-regulatory or co-regulatory approach to address most of these issues, whilst keen to maintain that the law offline applies equally online. This has meant that the UK has probably adopted less new legislation specifically aimed at addressing online problems than other countries.

An alternative approach is educating users of the Internet, especially children, so that they can protect themselves and be aware of the issues that may arise. There have been government campaigns, e.g. “Superhighway Safety”\(^11\) and the Home Offices ThinkUKNow site\(^12\), as well as child protection agencies’ own work, such as that of Childnet International\(^13\) and NCH\(^14\). OfCOM has a role to play in this also. The Communications Act 2003 sets out in s11 that it should bring about and encourage all aspects of media literacy. They are working with government and the industry to make sure that all areas of media literacy are addressed, be that via the national curriculum or via Internet safety events.

ISPs play a part in this role, both in terms of sponsorship and actual events, for example THUS plc through its Demon Internet brand works with Surrey Police as part of its Junior Citizens Events\(^15\).

And there are family friendly services that provide their own content, in a way that attempts to keep their users within a safe environment and where only web sites that are suitable are linked to.

---

\(^8\) http://www.bsc.org.uk
\(^9\) The Independent Committee for the Supervision of Standards of Telephone Information Services (ICSTIS) “is the industry-funded regulatory body for all premium rate charged telecommunications services”  
\(^10\) Specifically the Memorandum of Understanding which exists in conjunction with s46 of the Sexual Offences Act 2003 (http://www.opsi.gov.uk/acts/acts2003/20030042.htm)
\(^11\) http://safety.ngfl.gov.uk/
\(^12\) http://www.thinkuknow.co.uk/
\(^13\) http://www.kidsmart.org.uk/
\(^14\) http://www.nch.org.uk/itok/page.asp?auto=456
\(^15\) http://www.demon.net/aboutus/pressroom/2002/pr007.html
Further protection or limitation of access to unwanted material can be attained by using filtering, either at the ISP level or at the user level.

**Legal position affecting ISPs and notice and takedown**

The E-Commerce Regulations 2002\(^\text{16}\) limit the liability of ISPs for content they carry over their network and on their servers:

Regulation 17 “Mere Conduit” states that ISPs are not liable for material that they transmit across their networks provided they do not initiate the transmission, did not select the receiver of the transmission and did not select or modify the information contained in the transmission.

Regulation 18 refers to “Caching”. This section states that ISPs are not liable for material held in their caches provided they do not modify the material and adhere to the rules regarding the way caches work. They must also “act expeditiously” to remove any material from the cache once they are aware that the original item has been removed or a court has ordered its removal.

Regulation 19 “Hosting” applies the principle that ISPs are not liable for material hosted on their servers provided they do not have “actual knowledge” of the material and act expeditiously to remove it once aware of it.

Regulation 22 sets out what a court may consider as “actual knowledge”. Specifically, the regulation requires that:

- That the notice is served to the address as specified on the ISP’s web site
- The full name and address of the complainant is provided
- It is clear where the offending material is
- It is clear why it is offending

Although the E-Commerce Regulations provide some protection for ISPs there is still concern that they do not go far enough in setting out who can give “actual knowledge”. This is an important issue as, other than the Internet Watch Foundation dealing with child abuse images, criminally racist and pornographic material, there is no real authority for putting ISPs on notice. In the main, this is because other types of material are less noticeable, meaning that it is not always as easy to determine whether the material is illegal or not, which is why it would be up to a Court to decide whether someone has broken the law.

\(^{16}\) Statutory Instrument 2002 No. 2013
This position puts ISPs in an onerous position, as they can be put on notice by anyone, not knowing the real intentions of the complainant, but having to be “judge and jury” as to whether the content should be removed or not.

**Web blocking**

The first UK ISP to go public with a large scale website blocking system was BT in 2004. BT’s “cleanfeed project” takes a list of URLs provided by the IWF which it then blocks its users from accessing.

The IWF is in a unique position in the UK because it is the only authorised agency that takes reports from the public of indecent images of children, analyses the material and then reports them to ISPs and/or the authorities. By handling these reports the IWF has collated a list of web site addresses of indecent images of children and pay per view sites offering child abuse images.

One of the services the IWF offers to its members is access to this list in the form of a database of child abuse website URLs. BT took this database and provided a filtering system on their network for their retail customers. The IWF add between 3000 and 3500 website URLs to the database each year. The BT system is designed to prevent 'casual' users obtaining child abuse images from any of the websites in the IWF’s database by blocking IP addresses and individual pages.

It is believed that a number of other ISPs have followed suit and now operate a similar blocking system for their customers. Also, a number of web filtering companies offer tools that utilise the IWF’s list which ISPs can plug into their network, and even mobile operators have made use of the list.

The main purpose of any blocking system is to block access to certain types of material. The Cleanfeed system does this using the IWF’s child abuse URL database, in an attempt to prevent users accidentally accessing illegal images.

In China the government blocks a range of different types of material from education sites, material relating to democracy, Tibet, to sexually explicit, etc. Something similar operates in Saudi Arabia and other regimes exist in countries like Singapore.

---

17 by the Sexual Offences Act Memorandum of Understanding  
18 IWF 2003 Annual Report  
19 e.g http://www.webminder.net/  
21 See Documentation of Internet Filtering in Saudi Arabia, Jonathan Zittrain and Benjamin Edelman, Berkman Center for Internet & Society, Harvard Law School http://cyber.law.harvard.edu/filtering/saudiarabia/
Unlike China and Saudi Arabia there is no UK government censorship of the Internet. Unlike Singapore the UK government does not direct ISPs to block content it believes is “objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws.”

So there is no legal requirement for ISPs in the UK to block websites, and they are protected from liability under the E-Commerce Regulations. However, ISPs are continually looking at ways to provide a better Internet experience for their users as well as protecting the vulnerable.

How the blocking is done will vary depending on the system and the requirements. There are three main ways in which content can be blocked: at an IP level, obscuring DNS and blocking specific websites.

Each system has advantages and disadvantages. Blocking by IP could render whole servers blocked meaning that innocent websites which happen to share the same server as an illegal site, are also blocked; obscuring DNS (or DNS poisoning) suffers from the same problems; blocking specific websites is more accurate but may be more costly to implement.

**Does blocking work?**

So far web blocking in the UK has only been used to prevent access to illegal images of children. The real questions are whether it is effective at doing this and whether it could be used for any other type of material.

The short answer is yes, the blocking systems currently in place do work in that they prevent access to websites identified by the IWF as containing illegal images. For the casual Internet user this will probably be sufficient because they won’t be actively seeking out the material. For parents concerned about what their children may have access to the blocking also works. But as a means of preventing paedophiles deliberately obtaining illegal material it is less likely to be effective, because there are strong incentives for both suppliers and consumers to find ways of circumventing the blocking. Various countermeasures to blocking have already been identified, ranging from deceiving the IWF, to rerouting their connections via proxies, to discrediting the blocking system. Alternatively, paedophiles may simply be displaced to other distribution channels such as spam advertising or peer to peer systems.

Of course the effectiveness of a blocking system is only as good as the list provided. Although the IWF’s list of websites containing illegal material is well regarded, the IWF would never claim that their list is exhaustive. It will only contain those sites that the IWF is aware of, and new sites are continually being created. This is an important message to

---

22 Section 4 of the Internet Code of Practice (http://www.mda.gov.sg/medium/internet/i_codenpractice.html)
get over to the casual Internet users who may think that the blocking that is in place is flawless, when the truth of the matter is that it may only filter a subset of the material and that other filtering is required. Furthermore, it clearly means that “I assumed it must be legal because my ISP let me see it” is unlikely to work as a defence in court.

As to whether such systems can be extended to block other material, it is difficult to see how this could be effectively managed. This is likely to be why most ISPs who have implemented a web blocking filter based on the IWF list are reluctant to extend their blocking to any other types of material. They are aware of the limitations and complications will arise because of the law in terms of deciding whether material is or isn’t illegal and who maintains an accurate list of what should be blocked? Judges, ISPs, the government, rights holders?

**Obstacles to adoption of blocking**

One potential obstacle to widespread adoption of blocking is the cost. It is currently unclear how ‘scalable’ current solutions are, i.e. whether small ISPs would face the same cost per subscriber as large ISPs such as BT, or whether the costs per subscriber would be dramatically higher. As with any new technology, the costs are likely to fall with time, and it seems likely they will become affordable for most ISPs, especially if they can implement the changes on their own timescales, e.g. as part of wider system upgrades.

A related consideration is the strength of demand from consumers for such blocking, particularly if such demand is manifested by a willingness to pay (or to move to competing ISPs who offer the service). Market research\(^{24}\) has shown a clear willingness to pay for protection against spam, viruses and other annoyances, and indeed many ISPs are now using this in their marketing as a differentiator. However, there is currently little evidence of willingness to pay for protection against accidental exposure to illegal material. Where consumers do wish to purchase blocking services, it is generally against a much wider range of material deemed inappropriate either by parents or employers. Blocking of illegal content is a ‘nice to have’ but not currently something that subscribers will pay more for or that ranks high in their choice of ISP.

Where blocking has been introduced to date, it appears to have been largely motivated by considerations of corporate brand and positioning (protecting children from accidental exposure fits with a family-friendly brand), and a desire to be seen to acting in a socially responsible way (even if the true effectiveness in protecting children from abuse is far less than campaigners may suppose). There is no compelling business driver as there is in the case of spam, but as the internet permeates more and more of our daily lives, there is growing public pressure on ISPs to be more proactive in making the internet safe. As technology convergence breaks down the traditional barriers between broadcast entertainment and entertainment delivered over the internet, there will also be growing pressure on ISPs to be more proactive in regulating content.

---

\(^{24}\) Gartner – Consumers annoyed by increasingly hostile Internet Environment
A further concern is where the blocking stops. For some the mere fact that indecent images of children are being blocked is enough, for others there are many more uses that blocking could be put to. Given that most material considered offensive or illegal is hosted outside the UK, the biggest advantage is the filtering of foreign web sites which may exist because the material is not illegal or offensive in those countries or the material cannot be taken down so quickly, plus they are not affected by any agreement the government, law enforcement, stakeholders, etc. may have with the ISPs in the UK.

As an example, consider the concern of UK banks. Although there is a notice and takedown agreement between APACS and UK ISPs for the take down of phishing websites, this is pretty ineffective as most of the sites are hosted outside the UK. However, if they are hosted in say Russia, getting them taken down is harder, the authorities are less speedy in co-operating and the ISPs don’t have such a good relationship with law enforcement as they do in the UK. Just reviewing the IWF’s statistics for pay per view child abuse image sites is reflective of this fact: 31% of material has been traced to Russia.

It would therefore be beneficial to APACS for ISPs to block phishing sites which they would be more than willing to provide the URLs for. And surely the fact that this would limit the number of banking customers duped by such scams, this must a good reason to block these sites – so if ISPs are doing it for child abuse images, why can’t they do it for phishing sites. Phishing sites also are perhaps a more obvious type of material as the banks would be able to identify whether the site is theirs or not.

A further example is that of blocking material covered by court injunction. From time to time courts issue injunctions to block the publication of certain information (e.g. James Bulger’s killers’ identities, location of Maxinne Carr, pre-published information on Harry Potter books, etc.). If such injunctions can be issued with the Internet in mind, surely blocking systems can be adapted to uphold the injunctions and of course if ISPs with blocking systems are served with an injunction, they could easily find themselves in contempt if they did not carry out the wishes of the injunctions.

So, if there are possibilities for these two examples, what about other types of undesirable material? Websites that advocate suicide, encourage anorexia, defamation, copyright infringement, for example. There is great pressure to prevent access to such sites. They too could be added to the blocking list.

---

25 APACS is a trade association for institutions delivering payments services to end customers (see http://www.apacs.org.uk/)
26 Phishing is the act of tricking Internet users into giving out personal information. It has particularly been a problem of late for online banking: lots of spam emails are sent out alleging to be from a bank stating that the user’s bank details have been lost; they are then directed to a bogus website (that looks like the banks site) and the details are written a file and then used to commit fraud
27 IWF 2004 Annual Report
Although BT say that their Cleanfeed system can strictly only process the IWF database, the question still remains. If they were able to produce Cleanfeed in the first place, surely if sufficient pressure was to be applied, it could be extended to block other types of material.

If such a list of desirable material to be blocked were to be produced and supported by ISPs, then the potential could be endless. The impact would be firstly that the cost at managing such a list of web sites would increase as the list gets longer, as ISP’s networks would need to handle the redirections or dropping of Internet packets. This could well put smaller ISPs out of business or cause them to lose their edge over the bigger suppliers who can promote these services to attract customers. Furthermore, it could easily become a PR nightmare for any ISP who doesn’t provide such a service. Secondly, there is a fear that the UK would move further and further towards censoring what its Internet users can see on the Internet. Plus, because of the issues of notice and takedown already highlighted, it would have to be clear exactly who can put an ISP on notice and what would be added to a blocking list and under what circumstances.

Although the financial implications could be big for smaller ISPs there are perhaps some more technical issues that need resolving also.

One worry is that by interfering with the IP traffic across its network, the ISP will lose its mere conduit defence under the E-Commerce Regulations. Regulation 17 "Mere Conduit" states that ISPs are not liable for material that is transmitted across their networks provided they did not initiate the transmission, select the receiver of the transmission and did not select or modify the information contained in the transmission.

If an ISP’s blocking system redirects or blocks access to traffic on its network, it will be selecting the recipient and/or modifying the information. If this is the case then it is possible that the ISP would lose this defence. Once this defence is lost, third parties could exploit this vulnerability to pressure ISPs to block other types of material (copyright infringing, defamatory, etc) under threat of legal action. Small ISPs without the resources to fight legal battles could well succumb to such pressure.

Alternative approaches

The best way of preventing access to illegal material or even material that some wish not to see or would not want children to view, is to allow them to be their own censors. That way they can decide what they want to access (whether illegal or not) and with little cost or risk to the ISP. Indeed in the long run it may be cheaper to include a client side filter for its customers than to try and implement an effective blocking system, some of which will block known sites or even perhaps implement the IWF database.

Various filtering products exist from virus scanners, spam filters and content filters, all
packaged into “Internet Suites”. Such software is often offered with new PCs and some features are freely available.

The only problem with these though is user awareness. The old adage of adults having to get their children to programme video recorders because they couldn’t work out how to do it themselves probably rings true with Internet filtering software. Unless adults are able to set up their computers to protect their own as well as their children’s connectivity, often filtering products will be worthless.

A lot has to be done to educate parents as well as children about the dangers of the Internet and how to protect their families from them. OfCOM has a duty under the Communications Act to deal with the issue of media literacy. Although this can cover anything from helping people understand how to get the most out of technology to protecting them from the dangers, there is a lot they could do to send out messages to adults about how to be safe online. This will probably be cheaper in the long run, and probably more effective than individual ISPs implementing their own systems that are limited to blocking illegal images of children.

Furthermore, there is still a lot of work that can be done at a government level. Not in terms of legislation but in terms of trying to address the real problem.

Child abuse image sites exist because there is a demand for them. The issues the government should be looking at are why so many sites exist in the US (40% according to the IWF 2004 Annual Report) and Russia and what can be done about getting them taken down.

Conclusions

ISPs are confronted on a regular basis with the issue of what to do about material which may be illegal or offensive to many. One of the clearest areas of illegality relates to child abuse images, and working through the IWF, ISPs have virtually eradicated the problem in respect of material hosted in the UK. Worldwide though this is not the case, and through a list of known paedophilia sites, some ISPs have started to block access to such sites for their users.

But web blocking of this nature can have two distinct purposes. Protecting consumers from accidental exposure to such material or thwarting deliberate attempts to access it.

As a way of protecting consumers, blocking is likely to be reasonably effective (assuming a reasonably comprehensive list of what to block is available), since the consumer has no incentive to circumvent it. However it is unlikely to be particularly useful to the consumer unless the blocking goes well beyond the narrow confines of illegal material. Parents and employers for example, will wish to block access to many other categories of inappropriate content, and it is possible that ISPs will start to offer user-configurable
network-level blocking as an alternative to filtering software located on the user’s PC. However, many would argue that PC-based blocking combined with education and awareness raising is the more effective approach at present.

As a way of thwarting paedophiles, the effectiveness is much less certain, since countermeasures will surely emerge and illegal activity will be displaced to other communications channels such as peer to peer. ISPs may also be reluctant to introduce blocking while there is uncertainty over the legal implications for their ‘mere conduit’ defence. In areas of serious public concern such as prevention of child abuse, voluntary blocking by ISPs may have a useful role to play, but only as part of a coordinated package of measures, and with realistic expectations as to its effectiveness.