

ippr Background Paper:

“The Approach to Internet Content Regulation in the Context of Child Abuse Images Online”

Introduction

In little more than a decade, the Internet has grown from an academic tool to a mass provider of information, services and entertainment for the general public. In the UK 53% of the population now have access to the Internet at home, while 96% are aware of a place either at work, school, in the library or by using a public access point where they can access the Internet.¹

Initially the Internet was most extensively used as a distribution tool, a “carrier” analogous to the post office, delivering data from one point on the ARPAnet to another. However, with the invention of the World Wide Web and the influx of previously off-line services to the digital environment, commercial and public interests have taken over.

During this period of transition, there has been constant debate as to what the Internet is and thus how it should be regulated. The initial regulatory regime focussed on the competitiveness of operators. The Office of Telecommunications (OfTel) regulated the internet insofar as the incumbent telecom (BT) had monopoly market share, to facilitate local loop unbundling (llu) or to provide for the commercially viable offering of unmetered dial-up Internet access. The over-arching aim was to achieve technological reach relying on ‘light-touch’ regulation to promote a competitive market. This regulatory regime remained in place til end 2003.

Thus the Internet entered the UK’s regulatory framework in terms of its technical characteristics and was considered in much the same context as other utilities. The regulation of Internet content has traditionally been outside the scope of any regulator.

The regulation of communications generally changed dramatically in 2003 with the convergence of the five existing regulators (ITC, OfTel, Broadcasting Standards Commission, Radiocommunications Agency, Radio Authority) into the Office of Communications. The Act which give statutory powers to Ofcom was deliberately kept technologically neutral in order to reflect the convergence of media to deliver services. However, Internet content was explicitly excluded from Ofcom’s regulatory remit except in the context of media literacy.

The Internet is still considered as one media. But if we consider different media types – publisher, distributor, broadcaster and common carrier – it is clear that the internet can be used as each. Any one with the limited technical knowledge required to build a web page can do so and thus ‘publish’ content. For some services, such as geosites, all that is required is an Internet connection; the web space is provided free. Similarly the Internet can be used to distribute printed material or photographs, and to broadcast services ‘on demand’ such as concerts and radio. It is also considered a common carrier for email, the contents of the World Wide Web and more recently, voice over IP (VOIP).

¹ Cabinet Office (2004), *Enabling a Digitally United Kingdom*, Report of the Digital Inclusion Panel

While the capabilities of the Internet fit these four models to differing degrees, the affordance of ISPs the status of 'mere conduit' under the E-Commerce Directive coupled with the regulatory legacy, has led to the Internet remaining characterised as a common carrier. The familiar refrain that what is illegal offline is illegal online is used to support this position insofar as it suggests there is no further distinction of content, and that going online presents no barrier nor any change to community standards.

However, this reading of the offline / online parallel presents two issues. First, common carriers traditionally transferred analogue content. For the most part, the Internet is used to 'carry' digital content. There is a significant difference in the capabilities of systems to read digital content as opposed to analogue. The Internet industry itself has introduced technology which enables blocking of content (CleanFeed) and filtering systems are available to self-regulate. This represents the vastly different public expectations of Internet service providers to those of the Post Office, for example. Secondly, the idea that community standards are transferred and that 'online' activity should not be considered outside of these give rise to a view of the Internet as a stepping stone or accessibility tool to an extension of the public sphere.

Is there a case for calling the Internet a public space, and if so, do different regulatory principles apply? Most definitions of public spaces include the right of everyone to enter, without paying an entrance fee, for example roads, public parks and pavements. In addition in a public space, only the general law applies. Further restrictions on behaviour, such as dress codes or time limitations are not normally applied. Most regulations that apply offline also apply online. One important difference is the offline presence of an indecent displays act which does not apply to the Internet.

There have been calls to extend the law in this respect and there has certainly been a period of legitimisation of content, with the Government pushing to get all Government services online and the majority of major companies publishing proprietary information on the Web, leading to a higher profile of the *public* online. But the Internet is fundamentally different to the offline world in terms of content delivery. Content is not 'displayed' as such; rather it is requested by the user. It relies on people 'pulling' content and controlling what they view. This is an important factor in considering the responsibilities of society as a whole in this area. To an extent, the Internet offers a 'shared experience' which would be expected of a public space but while access is afforded to all, it is exercised in isolation.

Still the proliferation of home use of the internet amongst families and particularly children led to a number of businesses offering internet access packages to this market. To appeal to such buyers and reduce fear of harmful Internet content, ISPs developed self-regulation regimes, including Acceptable Use Policies, which place restrictions on Internet use which generally go further than the law. This has in part served to increase public expectations of the Internet and technologies to enable a truly 'safe' experience.

Neither a simple media nor public space in the traditional sense, the Internet sits somewhere between the two. As yet such questions regarding its regulatory position have not been addressed in detail but will become more urgent as technology develops, both in the context of content regulation, and increased sophistication of delivery of services online.

This paper focuses on concerns regarding the presence of child abuse images online. Under the Child Protection Act, it is criminally illegal to have such images in your possession.

Child abuse images pose particular problems for the Internet industry, law enforcement and parents alike. While there is no direct correlative evidence linking viewing of such images online to committing actual abuse, it is nonetheless the case that ease of distribution has seen offenders in possession of 1 million images; more than would have previously been possible without the use of new technologies.

There have so far been several initiatives to attempt to fill gaps left by the ill-positioning of the Internet in regulatory terms. These initiatives have revolved around trying to reduce illegal content and activity on wide range of services including chat, newsgroups, pay-per-view and websites. The UK has led the international field in terms of self-regulation and UK hosted potentially illegal content has fallen from 18% in 1997 to less than 1% in 2003. In contrast, 55% of child abuse content is now traced to the US, while 23% is traced to Russia.²

Internet Service Providers and the Internet Watch Foundation

Although there has been a tendency to assume ISPs should be responsible for content held on servers, the e-commerce directive afforded ISPs 'mere conduit' status and concluded that they are only responsible for content of which they have 'actual knowledge'.

This legal framework has led to the development of notice and takedown systems, the most successful and well known of which is **the Internet Watch Foundation (IWF)**.

The IWF was set up by the trade association for ISPs, the Internet Services Providers Association (ISPA), in 1997. It was initially intended to simply provide a hotline for reporting child abuse images. However, in 2001 its remit was widened at the request of the Home Office to include criminally racist content and it now deals with this and potentially illegal adult pornography. Reports can be made to the IWF via a hotline and once a report is received, the organisation will investigate whether it is an illegal image, trace the host of the content and, if the host is in the UK, give them notice that the image should be removed. They will also notify law enforcement.

If the image is found to be hosted outside the UK, the organisation will contact the relevant international body. To facilitate regulation of such a boundary-less medium, the IWF was instrumental in setting up INHOPE, an International body of Internet hotline providers. INHOPE's members include groups from the USA, Austria, Spain, Belgium, Australia, Denmark, Finland, Ireland, Greece, France, Germany, Iceland, Italy, Holland, South Korea and Sweden.

While the IWF performs a function similar to law enforcement in this respect, it is not funded by the Government. The organisation has a subscription based funding system whose 'members' constitute ISPs, mobile operators, search engines, software and hardware providers.

² IWF Annual Report 2003

While the IWF is a very successful body and seen as a model worldwide, it is difficult to classify as an organisation: for example, it is often called a self-regulatory body yet the function it performs relates specifically to criminal activity and therefore does not fit the normal 'self regulatory' model. ISPs could not choose to ignore IWF notices, and thus exist outside of the 'self regulation' scheme, without risking criminal prosecution. It has occasionally been called a co-regulation scheme instead, which intends to represent its place as sitting somewhere between being a voluntary membership body and an extension of law enforcement activity.

Similarly, while the IWF is a membership organisation and relies on subscriptions to do its job, it cannot withhold notices from non-member ISPs. To some extent, everyone benefits from the work of the IWF whether you fund it or not. This has meant that 'responsible' members of the industry bear the cost of the scheme. It also means that, while the problem of child abuse image distribution is not connected to industry value / profit etc, the IWF's income is. During a period of consolidation within the industry, the organisations income was dramatically reduced as companies no longer had the means to contribute or went into liquidation. However, funding for the organisation is now at £ 700,000 per annum³.

In response to concerns regarding content availability on newsgroups, the IWF developed a list of newsgroups which repeatedly carried illegal content and / or whose names were seen to advertise the presence of child pornography within. This list is regularly updated and distributed to IWF members who are then advised to remove access to these groups. Note that ISPs are not obliged to remove access since the list does not constitute a notice of actual illegal content. While it is likely illegal content could be contained within, actual knowledge relates to actual content. However, few ISPs run a full newsfeed, so in reality most of the listed newsgroups are not carried in any case.

When the list was first developed, there was some objection that it would not do much for the protection of children, merely shift the content to other more reputable newsgroups and thus increase the chances of someone accessing in accidentally. In addition, the host location of the actual images is not being investigated so possessors of child abuse images are less likely to be caught.

Recently the IWF has developed lists of websites, using a similar ideology to that for newsgroups. This is again distributed to ISPs and can be used for blocking purposes such as BT's CleanFeed system.

Home Office Internet Task Force for Child Protection on the Internet

The Home Office Task Force was set up in 2001 in response to a report, *Chatwise, Streetwise*⁴ from the Internet Crime Forum, a group of ISPs, Government officials and law enforcement. The report considered ways to protect children who use online 'chatrooms', providing key safety messages and recommendations for enabling secure chatroom activity.

The Task Force later launched a major public awareness campaign, including cinema and radio adverts, which highlighted the fact that people you chat to on the Internet may not be who they say they are. Instances of children arranging to meet online, in some cases resulting in a sexual crime being committed, led the Home Office to develop developing 'grooming' proposals in the context of the Sexual

³ Internet Watch Ltd, Annual Accounts 2003 - 2004

⁴ Internet Crime Forum (March 2001), *'Chatwise, Streetwise – children and Internet chat services'*

Offences Act 2003 which intend to make it an offence to groom a child, whether online or offline, for the purposes of committing a sexual offence.

In addition, negative media attention led some chat providers, most notably MSN, to suspend chat services entirely. Other chat services employ 'moderators' who monitor chatroom activity to ensure young people are not asked for personal details or experience inappropriate advances.

The Task Force has two main aims: to make the UK the best and safest place in the world for children to use the Internet, and to help protect children the world over from abuse fuelled by criminal misuse of new technologies.⁵

The Task Force is Chaired by a Minister (currently Paul Goggins MP) and is a partnership between child protection agencies, internet industry representatives, law enforcement and Government.

The Task Force does not have a budget of its own, and has experienced some personnel changes which some have felt have impacted on its ability to make significant progress in the area of child safety.

Peer-to-Peer Networks

There has been increasing concern regarding the amount of child abuse images being distributed using peer-to-peer file sharing software. Peer to peer technologies create a network in which each computer has equivalent capabilities and responsibilities: it effectively removes the client / server relationship. The use of file sharing software has allowed paedophiles to gain direct access to the hard drives of other paedophiles computers without the presence of a possible third party monitor or moderator that may exist in chat rooms or newsgroups.

P2P has become increasingly popular as paedophiles believe it is harder for them to be traced using this technology. There is no requirement for credit card details to be entered, a significant perceived 'benefit' following Operation Ore, and paedophiles are not required to be part of a traditional password protected "ring". However, investigators are able to access shared folders, find out whether illegal content is present and then trace the owner.

The scale of P2P file sharing in such illegal images is difficult to assess. However, the number of images held in some cases has been in the region of the hundreds of thousands. This means that while it is possible to trace offenders, police resources do not match the scale of the problem. There has been comment that resources have been focussed on low level offenders, i.e. those that download the material, rather than the hardcore offenders who may be committing real time abuse and then distributing the images using these means.

Mobile Phones and Content

As new mobile technologies begin to take off in the UK, there is concern that paedophiles may use them to contact children, amongst whom mobile phone use is pervasive, and groom them for abuse. As far back as 2001, 88% of under fifteen

⁵ <http://www.homeoffice.gov.uk/crime/internetcrime/taskforce.html>

year olds owned a mobile handset⁶. Young people will increasingly be able use them to access the internet, email and send photos.

Legally, children are only allowed pre-pay phones, rather than monthly contracts. However, they can legally purchase handsets at any age, some of which are compatible with 3G services.

In response to these concerns, the major UK mobile operators (Orange, O2, T-mobile, Virgin Mobile, Vodafone and 3) developed a Code of Practice for 'the self regulation of new forms of content on mobiles'. It covers content such as visual content, online gambling, chat rooms and internet accessed. It does not include SMS or peer to peer.

Under the Code, the mobile operators will appoint an independent classification body which will develop a framework for classifying content that is unsuitable for users under the age of 18. Commercial content providers will be required to self-classify content and all content classified as 18 will have access controls attached. Such restrictions are intended to ensure the UK does not follow suit with Japan where more than 90% of child prostitution cases involved the use of internet enabled mobile phones⁷. It has also become apparent that dating sites, while intended for adults, are increasingly used as covers for paedophilia.

All major UK mobile operators are members of the IWF and operate similar notice and takedown procedures to ISPs.

Education Programmes

There have been numerous education programmes launched to highlight children and parents of the dangers that may exist online. These have come from many different organisations including charities, ISPs and the Government.

Educating users on how to protect themselves and their children is clearly an important part of making the Internet safe for young people. However, the range of messages released may have led to some confusion amongst parents and there is a danger that this will lead to children's home Internet use being restricted entirely.

The difference between parental perceptions of their children's use of the Internet and the reality is highlighted in the July 2004 report, *UK Children Go Online*⁸. While 57% of children say they have come into contact with online pornography, only 16% of parents think their child has seen pornography on the Internet.

It also appears some safety messages are not registering effectively. 46% of 9 – 19 year olds who go online at least once a week say they have given out personal information online, while only 5% of parents think they have.

A confusion of messages is also apparently experienced by teachers in schools; teachers report they are given too much information from too many sources, while the National Grid for Learning produced Internet Proficiency Scheme is sent out only

⁶ Pupil Research Initiative (summer 2001)

⁷ David Batty and Justin McCurry (Jan 2004), 'Children to be shielded from abuse via mobiles', The Guardian

⁸ Sonia Livingston and Magdalena Bober (July 2004), 'UK Children Go Online – Surveying the experiences of young people and their parents', ESRC

in response to direct requests. The problem is in part compounded by the tenuous place of media literacy in the curriculum.

This confusion clearly needs to be addressed in a co-ordinated and non-alarmist fashion in order for parents to be effectively involved in keeping their children safe online. Further education and advice is something parents themselves would apparently welcome: in response to survey questions regarding a parental 'wish list', 75% wanted better teaching of use of the Internet in schools, and 67% requested better information and advice for parents.

Such problems will be the future focus of the Office of Communications (Ofcom) which launched a consultation on media literacy in July 2004.

Law Enforcement

Law enforcement has two major problems in tackling paedophilia: one is resources and available expertise, the second is the cross-jurisdictional nature of Internet crime.

The issue of resources was publicly brought to light with Operation Ore, a major scale investigation led by the FBI. The UK police were handed a list of over 6000 UK citizens who had used their credit cards to access child abuse images online through pay-per-view sites. However, many of the investigations stemming from this remain incomplete due to a lack of hi-tech forensic resources in the UK. Of the 1000 police officers trained to handle digital evidence, only 250 are with computer crime units⁹.

The UK police force consists of 43 different forces each of which operate within a geographical boundary. The set up was designed to meet challenges of traditional crime happening in specific locations within constabularies. In the case of child abuse images online, a crime may be reported without the location of the offence being known first. A child abuse image may be downloaded within the confines of one force, but from a server located in another, posted by a person situated in a third. Investigation of such crimes is therefore confusing. The UK does have a National Hi Tech Crime Squad, but given the range of crimes it has to deal with, including phishing, denial of service attacks and general internet fraud, the organisation.

Technological Solutions

CleanFeed / Blocking

In 2003, teacher Jane Longhurst was murdered by Graham Coutts. It later transpired that her killer had regularly accessed websites containing violent pornography and necrophilic content. Following this case, there was significant pressure from Parliamentarians for websites containing illegal or harmful content to be blocked at server level; over 300 MPs signed Early Day Motions (EDMs) calling for such action.

In July 2004, BT announced they were to introduce a blocking system, called CleanFeed which returns a 404 error message when a user attempts to access a website named on a list produced by the IWF which has been found to contain child pornography. While the system records how many times access is attempted, no further legal or investigatory action is taken.

Three weeks after launching CleanFeed, BT reported access to 250,000 URLs had been blocked. This generated a great deal of press attention and seemed to indicate

⁹ EURIM – IPPR E-Crime Study (May 2004), Supplying the Skills for Justice

that, while the number of child abuse images hosted in the UK has fallen dramatically, attempts at access were higher than originally thought.

There has been some speculation however that the BT figures are not entirely reflective of the actual picture, that they may refer to several URLs linking pictures to one page for example, and so independent verification of them has been requested¹⁰.

The Cleanfeed system has faced the same criticisms that were levelled at the IWF's proposals on newsgroup blocking. Again, it is assumed that content will just move elsewhere and the IWF will be forever involved in a game of cat and mouse trying to ensure access to content is cut off. There are also concerns that such content will move increasingly to peer-to-peer networks, which do not have a central server and where the content is difficult to discover and trace.

There has not been time to assess what implications this will have on ISPs' mere conduit status but there is likely to be heated debate in the future as pressure groups demand other forms of illegal content, such as copyright infringing material, be blocked using a similar system. The e-commerce directive is due for review at the European Commission level and this may be considered then.

Filtering

In addition to network level blocking such as that operated by BT's CleanFeed system, users have the ability to install and run filtering systems to enable self-regulation of their own or their child's online experience. For example, some ISPs, particularly those aiming at the family market, offer 'walled gardens', a fairly restrictive type of filtering which allows access only to pre-screened sites usually available through channels offered on the ISP's portal.

There are also filters which aim to match keywords considered unacceptable, and block sites accordingly. However, such systems are often subject to the problem of 'false-positives' i.e. they block 'innocent' sites containing offending words, albeit in a legitimate context. Most recently this was experienced with the Houses of Parliament's filtering system when Parliamentarians were denied access to information regarding the Sexual Offences Bill.

In response to concerns that illegal material could be easily accessed through search engines, the IWF has been working with search engine providers to build up a list of keywords and trends in order to protect users from being accidentally exposed to illegal content. The aim is to eventually develop a system which can prevent access to illegal content through such means.

Filtering systems are available fairly cheaply but again parents' knowledge of them is relatively sparse. This has led to calls for hardware suppliers to provide such software at point of sale with an analogy drawn between computers and car manufacturers: no-one would expect to be sold a new car without safety features such as seatbelts etc included so why does the same principle not apply to computer purchases?

Labelling

¹⁰ http://www.theregister.co.uk/2004/07/21/ispa_bt_cleanfeed/

A major initiative to encourage online publishers' self-regulation of content was launched in 1999 with the Internet Content Rating Association (ICRA). ICRA provides a free of charge labelling system which aims to work internationally by using "cross-cultural language". It works by inviting web publishers to visit the ICRA website and complete a questionnaire. All the questions are of the 'yes / no' variety and cover the presence of nudity, sexual content, inappropriate language etc. Once the questionnaire has been completed, the ICRA system generates a PICS label which can be added to the meta-tag of the website.

Parents can set access restrictions in accordance with the ICRA labelling questionnaire and the system will filter content accordingly. This will only filter access to content that has been actually labelled as inappropriate although parents are given the option of filtering all non-labelled content.

International Methods

National Centre for Missing and Exploited Children (USA)

In the US, the equivalent Internet hotline, the CyberTipline, is run by the National Centre for Missing and Exploited Children (NCMEC) which was established in 1984. While not part of Government, the NCMEC does have congressional mandates and the majority of its funding (\$31million dollars of \$40million dollars) comes from federal government.

The organisation as a whole has a remit much wider than that of the IWF and serves as a clearing house of information about missing and exploited children, distributing photographs and descriptions of missing children worldwide and offering training to law-enforcement.

The cybersafety element of NCMEC's work again covers more ground than the IWF, though this is due to the vastly differing budgets at each organisation's disposal, in contrast to the IWF over \$6m dollars of NCMEC's budget are dedicated to cybersafety activities, as well as the different legal framework in the US. Using a telephone hotline, or Internet reporting, members of the public can report the possession, manufacture and distribution of child abuse images, online enticement of children for sexual acts and the sending of unsolicited obscene material to a child. Given the amount of spam a single email account can received delay (estimated around 15 emails), the IWF simply does not have the resources to deal with 'obscene' spam, though in the rare cases that paedophilia is promoted through spam emails they will of course investigate this.

Belgium

Under Belgian Law, the distribution of all pornographic material, whether printed matter, pictures, photographs or audiovisual matter, is punishable as public indecency. Commercial gain is not required. The Belgian Judicial Police offer an official national contact point, providing an email address, where the public can report child abuse images online. The Belgian public are also able to contact www.childfocus-net-alert.be using an online form, free emergency number, fax or letter. Any reports will be passed to the Judicial Police for investigation.

The Belgian Hotline is operated as part of Child Focus, the European Centre for Missing and Sexually Exploited Children, which has a counterpart in the UK

(www.missingkids.org.uk) but which specifically deals with missing children rather than reports of child pornography or the wider US remit.

Other harmful content

This paper has focussed on child abuse images online. However, there are other forms of potentially illegal or harmful content that the Internet industry and law enforcement have to contend with. The Obscene Publications Act 59 and 64 created an offence of possession with intent to commercially deal in articles which have a 'tendency to corrupt or deprave' persons who are likely to see or read it, usually interpreted as a 'normal' adult.

This is clearly a subjective test and in the past has been used to ban publications now considered literary classics, such as *Lady Chatterley's Lover*. To strengthen and make clearer the test, there have been calls for it to be strengthened to include the tendency to corrupt or deprave a child. However, rather than rely solely on this legislation to decide what can or cannot be published using their services, the majority of ISPs also ask their clients to agree to an Acceptable Use Policy which often includes requirements that go further than the law and include clauses on offensive or indecent material. Some also require online publishers to include clear warnings of adult content to prevent accidental access by children.

In addition, the IWF deals with reports of extreme adult pornography.

Conclusion

Regulation of Internet content has thus far grown in a piecemeal fashion with many different stakeholders contributing to the regulatory and education framework. As long as we hesitate to arrive at a definitive vision of what the Internet is, this will be the case. In fairness, such an approach has not been unsuccessful and the UK is indeed one of the world leaders in terms of tackling illegal content online. However, as the expectations of the public for safer Internet use grow, and internet service providers are driven by commercial and political demands to reduce not just illegal but also undesirable or harmful content, the nature of responsibilities online will begin to change. Government and Industry should be aware of this before introducing further regulation, whether self or statutory, in this area.