

July 2005

Protecting Minors from Exposure to Harmful Content on Mobile Phones

EICN
*EUROPEAN INTERNET
COREGULATION NETWORK*

I. Introduction

The [Recommendation 98/560/EC](#) on the protection of minors and human dignity in audiovisual and information services, adopted on 24 September 1998, is in the process of being revised by the European institutions. As its first contribution to the on-going debate around this revision of EU policy, the European Internet Coregulation Network (EICN) recommended in its first policy statement that European policy makers, members of the industry and users should aim at making the next-generation mobile Internet a secure environment for children¹. In issuing such a recommendation, the EICN designated child protection in multimedia online mobile services one of its priorities for action.

In order to build on this contribution, the EICN tasked the Oxford Internet Institute (OII) to lead a working group examining the child protection implications of Internet-enabled mobile phones and other new mobile devices, part phone and part handheld computer. The working group attempted to gather information on the best practices of local mobile phone operators, content providers and distributors on a European scale, in part using information provided by other EICN members and their contacts in response to a project questionnaire of August 2004. The researchers also conducted exploratory interviews with industry representatives from the major network operators in the UK and regulatory and Parliamentary actors.

Based on this original research and on previous work conducted at the University of Oxford for the Safer Internet project www.selfregulation.info², the OII has elaborated a comprehensive project report on the "Implications of the Mobile Internet for the Protection of Minors", to be published soon after the release of this document.

The following report serves as a summary of that project, and concludes with the EICN's recommendations, which were unanimously adopted by the member organisations on 28 July 2005.

¹ European Internet Coregulation Network. 2004. *Child Protection on the Internet. Preventing the Exposure of Children to Harmful Content. A Political Statement.*

² Ahlert, Christian, Alexander, Marcus & Damian Tambini. 2003. *European 3G Mobile Industry Self-Regulation: IAPCODE Background Paper*, Paper delivered at the World Telemedia Conference, Prague.

II Background

The launch of third generation mobile networks (3G) across Europe in 2003/4³ has highlighted the emergence of mobile Internet access, even though a more limited form of Internet access was previously possible under narrowband networks and in more developed mobile markets in East Asia. In the autumn of 2004 most of the major UK network operators began to offer handsets which are capable of using 3G for connecting to online services, a phenomenon mirrored elsewhere in Europe. More recently, further developments in handset technology brought new devices onto the market capable of seamless roaming. These handsets can switch automatically between different networks including wireless local area networks (LANs), a feature which further blurs the already muddy distinction between mobiles-accessed Internet and ordinary wireless access from a PC or PDA.

It is important to note that despite the fact that concerns about mobile content have been stimulated by the emergence of 3G and 'Internet-enabled handsets' for the purposes of this report, mobile content covers three different types of content: commercial content provided by mobile operators and largely purchased from third party suppliers; content available on the public Internet; and also content produced and passed through peer-to-peer communications such as photos. Differentiating between these three types of content is important as even if they are a source of common concern, different technical or regulatory responses are possible and potentially desirable in each case.

Mobile phones are thus becoming an ever more sophisticated device for accessing email, the Internet and other services. Such technological advances have however also led to the development of new business models for network operators, which focus largely on collecting revenue from online content. The models include:

- (1) network operators offering their own content,
- (2) network operators allowing third parties to provide content,
- (3) networks providing open access to the Internet.

Far from being mutually exclusive, these business models are increasingly combined by operators in a single strategy. Indeed, in the UK at least, mobile operator 3 is, as of June 2005, the only operator not offering *any* open access to the Internet, whether subscribers want it or not. It is important to recognize the existence of these different models however, as the possibilities for co- and self-regulation associated with the content delivery model will clearly vary according to the sources of content.

It is also important to remember that it is not just consumers who will benefit from these advances: most market forecasts see adult services, as well as gaming and gambling services, potentially offering a significant source of revenue for network operators. In this light any workable self or coregulatory framework must balance concerns for child protection with those of economic competitiveness.

³ The first European 3G networks were launched in the Isle of Man off the UK mainland in 2001, but national commercial roll-out was begun by 3 (Hutchison 3G) in Italy and the UK on 3rd March 2003: see <http://www.phonescoop.com/news/item.php?n=487>

III Mobile Content – the State of Play

Mobiles vs PCs

Just because mobile technology has developed to the point where Internet and commercial content are easily accessible does not mean that such phones offer the same risks to children in terms of harmful material as access to such content via PCs. In particular, there are relevant differences in the way that the devices are designed, sold and used which need to be taken into account in order to understand the nature of public concerns and to design a policy response accordingly. These differences can be summarised as follows⁴:

1. **Ubiquity**: given the increasing pervasiveness of colour screen technology in even standard mobile phone models, many secondary and even primary school students are likely to have phones with colour screens at the birth of the wireless Internet, whilst most children have only gained access to the Internet via PCs at a later stage in that technology's development.⁵ Although it is not yet clear that many children use their phones to access the Internet or commercial content (for example see Vincent 2004), the high levels of mobile phone ownership mean policymakers should not be complacent.
2. **Supervision**: unlike PC-based access to the Internet, mobile use is, by its very nature, more likely to be private and largely unsupervisable. This may be tempered to some extent by the possibility of parental monitoring of itemized phone bills, although in the UK as elsewhere in Europe, large numbers of mobile users have Pay-as-you-go accounts, with under-16s especially likely to have such accounts.
3. **Control**: with PCs, access to the Internet is provided and controlled by an Internet Service Provider (ISP) and users can choose which ISP they contract with after buying their PC. Such choice and competition amongst ISPs means that individuals could easily opt in or out of various filtering options by shopping around amongst ISPs. In the case of mobile-accessed Internet, however, a handset is usually bought as part of a contract with a particular operator. Even if it is practically possible to change network, this is not something which many customers would do on a regular basis. So long as this remains the case (and it may change) it is easier for network operators to adopt content controls, such as filters, as at any point in time they are the only gatekeeper to the Internet for individual users of their services. This feature, combined with the different models for content delivery described above means that mobile network operators can and do provide so-called 'walled gardens', which effectively limits Internet access to content approved by the network operator.
4. **Filtering Defaults**: it was widely expected that on mobile phones, filtering defaults when available would largely be opt-in, unlike opt-out Internet Explorer, AOL and Google, meaning that 2.5/3G mobile phone users would by default have access to adult content. In the UK, this position has largely been reversed, in no small part due to lobbying by child protection groups, meaning that those purchasing new mobile phones will now usually need to opt out of filtering applications, which will only be possible after age verification.
5. **Convergence of Capture and Distribution in One Device**: most devices now offer digital image capture capabilities and also enable distribution of these images via the network, and locally at no cost by infrared and Bluetooth - picture messaging

⁴ Categories adapted and extended from Marsden (2004).

⁵ Figures from the UK Department for Education and Skills show that in 2002 41% of children between 5 & 18 owning a mobile phone, a figure which is likely to have increased still further in the past two years (DfES 2002). A recent consumer survey suggested that mobile phones are owned by over 5 million under-16s in the UK (Mobile Youth 2005).

is an example of this. This means that in principle, the distribution of inappropriate pictures, or even pornography is only 'One Click Away' from digital image capturing; but in a way that cannot be controlled by filters at the network level.

6. Peer-to-Peer File Sharing: Given that 3G bandwidth is still much slower than standard broadband connections, p2p file-sharing of photos, movies or music is time consuming and costly. However, as operators are now starting to offer seamless roaming packages whereby mobile phones can be used at home with standard wireless broadband connections and on the move with wireless hotspots, P2P may further drive usage of mobile-accessed Internet by children.

Harmful Content?

One of the most difficult issues that arises in relation to the protection of minors from inappropriate content is at what age children should be able to access different types of content, or indeed what counts as 'inappropriate' or 'harmful' content for different groups of users. In many cases, for example, material might be deemed inappropriate and potentially harmful for a 7-year old, but harmless for a 16-year old. In addition what is deemed harmful in the UK for a 16-year old may be seen as entirely appropriate in the Netherlands, or Sweden. Any workable code of practice would have to address these issues within the context of its own cultural and regulatory norms, thus the Network has avoided making any statement as to what constitutes 'harmful content' for any particular country.

The Network has chosen to focus on harmful or inappropriate content, as illegal content, such as child pornography or hate speech, is (at least in Europe) less controversial because it is widely agreed to be unacceptable, and is explicitly prohibited by the national law of many EU member states and a corresponding network of resources, such as national hotlines, already exists to deal with it.

Inappropriate content for under-18s potentially includes, but is not limited to the following:

- Pornography
- Violent games
- Unmoderated chatroom services
- Music with sexually explicit lyrics or videos
- Spam containing adult content
- Gambling

Other concerns not relating to content may also be raised, for example, concerns about the cost of premium rate services which under-18s may choose to use such as interactive voting, or ringtone downloads but such concerns are beyond the scope of this report.

Should children's access to mobile content be a policy concern?

As has been pointed out above, while mobile phone use by its very nature is less open to physical supervision than PC use, there are certain technical features of mobile phones which would suggest that the risks to children are potentially more controllable than those posed by PC-accessed content. The role of network operators as de facto gatekeepers means that there is a single bottleneck through which access to commercial content and the wider Internet can be controlled. This feature, combined with the fact that unlike most PCs, mobiles tend to be used or owned by a single individual, mean that in principle at least, there is more scope to sell or modify handsets in such a way that they are set to disallow access to material unsuitable for children. These caveats notwithstanding, the media have carried ever increasing numbers of sensationalized

stories surrounding children's use of mobile phones since start-2004. In the UK, stories have included coverage of:

- schools and leisure centres banning the use of camera phones for fear of paedophile exploitation;
- the possibility of child abduction as the result of information provided by new location-aware handsets and
- accounts of a sex-offender who lured girls for underage sex through the use of Internet chat rooms (BBC news website, January-October 2004).

Market surveys have revealed potentially mixed feelings on the part of parents when it comes to their offspring's use of mobile phones. The National Children's Homes charity in the UK recently reported that 86% of Scottish parents feared that 3G mobile phones could threaten the safety of their children, whilst at the same time, the number of UK 7-10 year olds with mobile phones doubled in three years (2001-3), with parents' concerns about their child's safety being cited as one reason for this (source: Mintel survey, reported BBC news 28/4/04). With the advent of 2.5 and 3G phones, it would seem as if mobile phones might be perceived by parents as, on the one hand, helping to secure their children against abduction, yet exposing them to other new dangers of theft and inappropriate Internet content on the other. It is important to bear this trade-off in mind when looking at possible measures for child protection – the Internet potentially offers many benefits to children, educational, cultural and social, and any proposed solutions should work to ensure that access and information rights are preserved to the greatest extent possible whilst balancing for other concerns.

There is as yet little academic research on children's use of Internet-enabled mobile phones. One very recent study seems to offer little evidence to suggest that children make significant use of their mobile phones to access the Internet or download commercial content, and price sensitivity is cited as one important explanation for this (see for example Vincent 2004). But given that the technology and pricing plans are changing rapidly, further research is needed to determine whether this will remain the case as 3G handsets face and pass their first anniversary in Europe.

Given the limitations of current research on mobile accessed content it is worth looking also at some of the studies of children's use of PCs. The European SAFT survey found that between a quarter and a third of 9-16 year olds had been accidentally exposed to violent, offensive, sexual or pornographic content in 2002/3. Sonia Livingstone's 2004 UK survey of children and Internet use backs this up, finding that 36% of 9-19 year olds have found themselves on a pornographic website when looking for something else and 25% say they have received pornographic material via junk mail (Livingstone 2004, p.29). Interestingly though, Livingstone's survey also examined parents' assessment of their children's online experiences, which showed that children report much higher levels of problematic experience online than their parents appear to be aware of. This would suggest that media and policy exhortations to parents to supervise their children's use of the Internet on home PCs may not be sufficient presently to deal with the problem of access to inappropriate material. Whilst there is clearly still room for effective and universal media literacy training, given that children's use of mobile phones is by its very nature so much harder to monitor and supervise, this finding also suggests that in the case of mobile content, technical and self- or coregulatory measures do indeed have a significant role to play in protecting children from inappropriate content, as will be outlined shortly. At the very least it also suggests that significant media literacy and awareness raising efforts should be directed at children, not just parents and carers.

IV. Possible policy responses?

There are a range of different regulatory options available for dealing with these issues, each with their own advantages and disadvantages. Proponents of self-regulation claim that this is the most effective and efficient form of regulation in a fast-paced and complex market such as that enjoyed by the mobile phone and Internet industries. The "self" in self-regulation usually refers to an industry which is developing rules and codes of conduct for itself. Enforcement and monitoring of the regulatory environment in this model usually also lies with the industry itself. Observers of self-regulation usually cite the threat of government intervention as the main motivation for industry's development of self-regulatory codes, as this could make doing business much more costly. In reality, however, "pure" self-regulation, with little or no role for government, is almost never found. Even in the Internet and mobile industry where direct regulation of content is almost entirely absent, there is a multitude of national laws ranging from the protection of minors in general, to freedom of expression and copyright, which effectively regulate Internet content, or any content delivered to mobile Internet devices.

Throughout the 1990s self-regulation was heavily advocated by the European Commission, most notably under the Safer Internet Action Plan, but this approach seems to have fallen somewhat out of favour with recent measures promoting a more "coregulatory" approach. Whereas "self"-regulation implies a degree of independence from direct state regulation, "co"-regulation implies that the private companies, the state and user-groups are involved in jointly developing rules and regulations. This might be thought more desirable to the extent that research on self-regulation has shown that some self-regulatory models in the Internet industry lacked proper procedures for oversight and enforcement, and amount to little more than declarations of good will.

Coregulation in this regard is a new process of elaborating rules in a world of "shared responsibilities" between all the actors. According to the European Internet Coregulation Network, coregulation aims at organizing a cooperation process on rights and usages issues between public authorities, the private sector and the civil society. Through this cooperation process, the actors have the opportunity to reach a consensus point on each subject. Coregulation allows to combine regulatory tools and preferences at the disposal of each actor (laws and decrees, codes of conduct, technical tools, self-awareness)⁶. Given the nature of this relationship, there are of course different possible models of coregulation which allow relatively greater or lesser degrees of freedom to industry, more or less involvement from consumer bodies and implication of the state. Thus, for example, as the OII observed in regards to mobile content, the United Kingdom's approach can be described as more self-regulatory as government involvement is fairly minimal, whereas in Germany and Italy for example it is stronger. It is also conceivable that a coregulatory process of consultation and negotiation might produce a framework such as a code of practice within which certain activities are left to be regulated by industry (such as provision of filtering tools or age verification processes) whilst others (such as the classification of commercial content) are subject to regulatory standards or the oversight of an independent monitoring body (as in the UK).

The European Commission has reported on Member States' regulation of mobile phone content and recommended a coregulatory approach where possible, although as that report indicates, some Member States do have applicable legislation which covers mobile content. It can be expected that the European Commission will return to the subject matter as part of the continuing Safer Internet Action Plan, which primarily aims at promoting awareness amongst member states of issues around child safety online,

⁶ See European Internet Coregulation Network, *Policy Statement on "Internet Governance"*, July 2005.

indeed a "Safer Internet Forum" on "Child Safety and Mobile Phones" bringing together stakeholders from all over Europe was held in Luxembourg on 14 June 2005.

The EICN's working group reported on several different strategies for dealing with child protection and mobile phones which are employed in Europe to regulate commercial content accessible via mobile phones and sometimes secure Internet-connectivity through mobile networks:

- *Germany*: introduction of legislation which establishes consistent standards for the evaluation of identical content across media sectors "irrespective of the mode of transmission". A single supervisory body - the "Commission for the protection of minors in the media" (*Kommission für Jugendmedienschutz* – KJM) - has been created for broadcasting, the Internet and other forms of digital media in regard to the protection of minors and human dignity.
- *United Kingdom*: establishment of a Code of Practice which all six mobile operators have signed up to which introduces specific measures to protect children from accessing harmful content inadvertently.
- *Italy & Ireland*: introduction of mobile codes of practice which include some measures to protect children amongst other commitments, although only in Italy did government play a significant role in helping to develop and promote the Code.

The UK Code of Conduct was of particular interest to the Network as it is so far the most detailed and thorough measure introduced to deal with the issue of child protection and harmful content accessed via mobile phones.

The UK Code

The UK Code was drafted by a committee including all six UK network operators and virtual operators (3, Vodafone, Orange, T-Mobile, Virgin Mobile, O2). Informal consultation with content providers, infrastructure and handset suppliers and government at national and European Commission levels took place. The six operators include all four of the largest pan-European operators⁷. Details of the Code's implementation (see below) were announced on 7 February 2005 with the launch of the Independent Mobile Classification Body (IMCB)⁸. The Code itself is unremarkable, but its ex ante adoption, prior to many adult services being known to the general public, is exceptional and reflects high awareness in the sector both of potential harms and of the value of self-regulation. In part, this can be attributed to the market size and regulatory resources of the four giant companies behind the drafting.

The main points of the code are:

- All commercial content unsuitable for under-18s will be classified as "18", and will only be made available to customers when the networks are satisfied that the customer is 18 or over.
- The classification framework will be comparable to those applied to other media, and will be created by a body independent of the mobile operators.
- Chat rooms available to under-18s will be moderated.
- Parents and carers will be able to apply filters to network operators' Internet access service to restrict the content available via a particular phone.
- Mobile operators will work to combat bulk and nuisance communications.

⁷ 56% of the 2000 European subscriber market was O2, Vodafone, T-Mobile and Orange – TIM and Telefonica Moviles, with less significant interest outside their domestic markets, are small in pan-European terms. See Ahlert et al (2003) at p4.

⁸ See Classification Framework at <http://www.imcb.org.uk/assets/documents/ClassificationFramework.pdf>

In addition, the Code observes the same 'notice and take-down' requirements with regard to illegal material as those applying to fixed-line ISPs. Thus Section 3 of the Code states:

"Mobile operators will work with law enforcement agencies to deal with the reporting of content that may break the criminal law. Where a mobile operator is hosting content, including web or messaging content, it will put in place notify and take-down provisions."

There are, however, several restrictions on what the Code does or should cover. For example, the UK Code explains that:

"The Code covers new types of content, including visual content, online gambling, mobile gaming, chat rooms and Internet access. It does not cover traditional premium rate voice or premium rate SMS (texting) services, which will continue to be regulated under the ICSTIS Code of Practice."⁹

This is explained by the fact that an effective code of practice and regulator (ICSTIS) have been in place to regulate such content for the last twenty years, so no new action on this is necessary.

Similarly, the Code refers to wider Internet content not directly supplied by third parties to the mobile operator but notes that operators do not have control over this, and as such cannot be held responsible for its classification or the availability of adult material. Instead it states:

"Mobile operators will therefore offer parents and carers the opportunity to apply a filter to the mobile operator's Internet access service so that the Internet content thus accessible is restricted. The filter will be set at a level that is intended to filter out content approximately equivalent to commercial content with a classification of 18 "

Responsibilities here mirror those of fixed-line ISPs.

The code also does not seek to cover other issues which have already stimulated media concern such as the use of camera phones and Bluetooth technologies for content creation and distribution that does not require downloading from a website, or other forms of P2P file-sharing. To the extent that any form of regulation is possible with such content, this is already subject to nuisance call procedures and criminal laws which outlaw the transmission of illegal images and malicious communication.

Thus the Code covers the three different types of content outlined at the beginning of this paper, but ascribes very different responsibilities to mobile network operators in each case. In doing so, it covers most of the potential areas of concern for parents, and demonstrates to government that the industry has taken its corporate responsibility seriously, but does still leave unanswered some important questions. Issues include how to build a relationship of cooperation between mobile operators and commercial content providers, raising awareness of the code and the role of retailers. Also, the code is heavily dependent on age verification procedures which are still far from fool-proof and are open to fraud (although it could be argued that the primary responsibility of the mobile industry is to prevent accidental rather than deliberate access to adult material for minors.) It also still remains to be seen just how successful content rating systems will be. Content on the wider Internet will pose larger problems as it cannot be rated and restricted by mobile operators in the same way as commercial content. Therefore, it is

⁹ UK Code at p2.

likely that the most effective approach will be to combine the utilization of filtering software, content labels and URL block lists (Zittrain 2004).

It is also worth emphasising that in addition to the country-wide measures outlined above, there are many examples of self-regulation practiced by an individual network operator. In the UK, for example, both Vodafone and 3 have introduced additional measures: 3 by offering access only to a walled garden of rated content, and Vodafone by anticipating consumer concerns and introducing 'access control' measures which restrict access to adult content unless the user is over 18 and chooses to opt in. This self-regulating behaviour is particularly interesting in the context of large operators which operate in multiple national markets; thus Vodafone has introduced its content control systems not only in the UK where a code of practice exists but also in the Netherlands which lacks such a code.

It still remains to be seen whether child safety will become a key branding issue for mobile operators in the same way it has for fixed-line ISPs such as AOL, but it should at least be clear that business interests need not be harmed by the implementation of child protection measures; in fact there are tremendous gains to be made by operators who can show they have reduced the risks to children. With the global market for adult content on mobile handsets predicted to grow to around \$1billion by 2008¹⁰, mobile operators who are trusted to prevent minors accessing harmful content will be free to capitalize on the opportunities offered by highly lucrative adult services.

¹⁰ 'Child Protection Unlocks Wireless Adult Content Market.' Yankee Group study, released 25/10/2004.

V Conclusions and recommendations from the EICN

It is still 'early days' as far as control of harmful content accessed via mobile phones is concerned. Codes of practice have been introduced and limited public consultations held, but it remains to be seen how these solutions will work in practice, or how rigorously the codes will be applied by the mobile and content industries. Further, it is not yet clear how significant a risk will be posed to children by use of these phones, but it is important that policymakers be aware of the potential issues and are prepared to work with industry and consumers to prevent harm where appropriate.

On the basis of these various observations and against the backdrop of the analytical report prepared by the OII, the European Internet Coregulation Network draws the following conclusions concerning the regulation of commercial and Internet-based content:

1. That the various types of content and services which can be accessed via mobile phones may pose risks to minors and that policy responses to this issue should be considered.
2. That the European Commission and EU member states should monitor and learn from the operation of mobile codes of practice in the UK, Ireland and Italy & also fund or undertake research providing more information about children's use of mobile phones.
3. That coregulation, as the policy-making process involving industry, governments and user groups in the regulatory debate, is probably the most appropriate approach to this issue, as it offers the most scope for stakeholders' wishes to be taken into account, while also potentially offering more transparency in the application of the regulatory initiatives adopted than self-regulation alone. This leaves open the possibility that within an overarching coregulatory framework, the different types of mobile content might be subject to differing levels of regulatory or self-regulatory control, as is the case in the UK.
4. That members of the Network should, in accordance with the principle of coregulation, engage with industry, government and user groups in their own countries to discuss the appropriateness of introducing measures for protecting minors from harmful content accessed via mobile phones, and that the European Commission should do the same. Where appropriate, members of the Network should further endeavour to develop and promote a Code of Practice as a contribution to the coregulatory process in their own states.
5. Further, as issues of child protection and Internet access are a source of concern in many European countries, and as several of the largest mobile operators have a presence in more than one country, policy debates should be undertaken at the European, not just national levels. This would still allow individual states to determine what content should be available to which age group according to their own cultural norms.
6. The introduction of codes of practice would seem to be a suitable policy response to this problem when arrived at in a genuinely coregulatory manner and backed up, as appropriate, by the introduction of an independent body for monitoring and ensuring application of the codes.
7. As the basis for an international framework for child protection and mobile phones, the Network propose a common set of principles which national codes of practice could be built on:
 - The Internet and other forms of digital content are potentially of huge benefit to children for educational, recreational and cultural reasons. In order for this potential benefit to be maximised, children's inadvertent

access to harmful content should be minimised, and this applies to content accessed via mobile phones as well as PCs.

- Awareness-raising and media literacy training are key to empowering parents and children to use the Internet safely; both government and industry have responsibilities to bear on this issue.
- In order to support the restriction of certain content to users of particular age groups in accordance with countries' own standards of decency and appropriateness, content classification and age rating should be employed to control access to commercial content, and site blocking and filtering tools should be employed to limit access to wider Internet content.
- Independent rating bodies could have a role to play in classifying any content offered by the operators as premium services according to national standards and in adjudicating resultant disputes.
- Interactive services used by minors, such as chatrooms, should be moderated where appropriate.
- Handset manufacturers and network operators should continue to undertake research looking at new, more accurate and non-intrusive ways of managing access to content by minors through mobile phones, especially on the wider Internet.

References

Ahlert, Christian, Alexander, Marcus & Damian Tambini. 2003. *European 3G Mobile Industry Self-Regulation: IAPCODE Background Paper*, Paper delivered at the World Telemedia Conference, Prague. Available online at: <http://www.selfregulation.info/iapcode/031106-mobiles-revised-bckgrd.pdf>

DfES, 2002. *Young People and ICT 2002*, London: DfES. Available online at: http://www.dfes.gov.uk/ictinschools/uploads/genericdocs/Young_People_ICT_2002.pdf

European Internet Coregulation Network. 2004. *Child Protection on the Internet. Preventing the Exposure of Children to Harmful Content. A Political Statement*. Available online at: <http://network.foruminternet.org/IMG/pdf/childprotection-policystatement.pdf>

Livingstone, Sonia. 2004. *UK Children Go Online*, ESRC. Available online at: <http://www.children-go-online.net/>

Marsden, Chris. 2004. Is Peer to Peer the Next Mobile Regulation Challenge? Editorial for PCMLP Self Regulation Review, February 2004. Available online at: <http://www.selfregulation.info/iapcode/0402xx-selfregulation-review.htm>

Vincent, Jane. 2005: *Examining mobile phone and ICT use amongst children aged 11 to 16*, Digital World Research Centre, University of Surrey, available online at: <http://www.surrey.ac.uk/dwrc/People/Vincent.htm>

Zittrain, J. and Edelman, B. 2004. 'Documentation of Internet Filtering Worldwide', pp137-148 in Hardy, C. and Moller, C. eds *Spreading the Word on the Internet: 16 Answers to 4 Questions*, Vienna, OSCE

