

Promoting children's interests on the internet: regulation and the emerging evidence base of risk and harm¹

Sonia Livingstone, London School of Economics and Political Science

[s.livingstone@lse.ac.uk]

Brian O'Neill, Dublin Institute of Technology

[brian.oneill@dit.ie]

Internet, Politics, Policy, September 16-17, 2010, Oxford Internet Institute

Introduction

Advocacy for child protection online has tended to swim against the tide of a dominant liberal discourse concerning the internet which posits that either the internet should not be regulated or that it can't actually be regulated at all. Regulatory trends in Great Britain, in Europe and in the wider international arena have promoted regulatory arrangements whereby industries themselves with varying degrees of partnership or oversight by relevant state agencies practice 'light-touch' regulation based on codes established within industry fora with minimalist prescriptions on content and with ultimate responsibility for risk exposure shifted to the end user.

The dominant discourse of this regulatory approach is framed both within an economic logic which argues that impediments placed in the way of an emerging new media ecology will have negative consequences for competitiveness and economic

¹ Parts of this paper were previously presented at the *World Summit on Media for Children and Youth*, Karlstad (June 2010) and represent a summary version of a longer article published as Livingstone (in press), 'Regulating the internet in the interests of children: Emerging British, European and international approaches', in Mansell & Raboy (Eds.) *The handbook on global media and communication policy* (Oxford: Blackwell).

development as well as within a libertarian framework that gives primacy to adult rights to freedom of speech over and above ancillary issues of public interest. In this context, promotion of the interests of children online has met with significant challenges, and child protection measures are frequently viewed as a threat to privacy and freedom of expression rights.

However, this situation is changing. Regulation of the internet in some form is more and more accepted on an international legislative basis and issues of child online protection feature more prominently in debates about current and future internet technologies than heretofore. A host of inter-governmental organizations, internet technology and service providers, civil society groups as well as national governments themselves are increasingly preoccupied with the challenging dilemmas posed by balancing empowerment and protection of children and young people online. Our concern in this paper is to place the case for promoting children's interests on the internet in the context of wider debates about internet regulation. Firstly, we examine the framing of policy debates about online child protection within the context of prevailing approaches to internet regulation. Secondly, we highlight some of the emerging evidence regarding children's exposure to risk and harm online. Finally, in considering the policy and regulatory response to risk and harm on the internet for children, we suggest some of the structural or environmental issues that regulation might address, thereby minimizing risks to children while not compromising the very obvious opportunities and benefits that the internet affords.

Regulation and the internet

The promotion of internet infrastructure, access and use in the workplace, schools, communities and households has been a concern of governments across the world. Infrastructural, market and communications sector regulation has been the object of sustained political attention and investment for all western countries with the European Union engaged in intense competition with North America and the Far East to enhance its position as a global leader in advanced ICT (Lembke, 2003). Societal dimensions of such a policy framework are not ignored either and there is wide support for the view that a more inclusive information society is also a more competitive knowledge economy and that enhanced digital literacy skills contribute to

competitiveness, greater civic participation and a stimulus for a more pluralistic media sector (Commission of the European Communities, 2009). At the same time, Information Society policy has been characterized nearly everywhere by liberalization of the market place and a light-touch regulatory regime based on the belief that industries and market sectors themselves are best positioned to respond to the fast pace of change in information and communication technologies (Green, 2010). This reflects a wider shift in media policies towards more indirect and flexible forms of regulation away from top-down government measures, encompassing self-regulation by industry groups themselves as well as elements of co-operation or co-regulatory approaches with relevant state agencies (Jakubowicz, 2004; Freedman, 2008). In this context, governments have at different stages made various pronouncements that the internet would not be subject to the same kind of regulatory regime as traditional media industries. Thus, for example, the Canadian regulator, the CRTC, following a wide debate in 1999 declared that it was in the best interests of the fledgling new media sector and society as a whole not to regulate the internet (Canadian Radio-television and Telecommunications Commission, 1999). Similarly, Tessa Jowell, the UK's Culture Secretary, declared in 2006 that 'Because the UK's media sector and other creative industries are the jewel in our economic crown [...] the best approach is to rely as far as possible on self-regulation.' (Jowell, 2006).

Such pronouncements were in the spirit of the oft-repeated 1990s claim that the internet either cannot or should not be regulated (see, for example, Rheingold, 2000). Aiming to protect the experimental ethos in which it developed, and what Zittrain calls its 'generativity', the internet's ability to 'produce unanticipated change through unfiltered contributions from broad and varied audiences' (Zittrain, 2008), internet activists, civil libertarians and many others concerned with preserving the free character of the internet continue to adhere to this position. As Livingstone argues elsewhere, claiming that the internet cannot be regulated can be interpreted in a number of ways (Livingstone, 2010). It can mean, for instance, that we *should* not regulate the internet for reasons of freedom of speech and in opposition to any form of censorship. This appeal to keep the internet open and free is a well-established position best illustrated by First Amendment campaigns in the United States, most notably the attacks in the USA's Communications Decency Act 1996 (Nesson and Marglin, 1996) and in more recent opposition to debates on internet filtering (McNamee, 2010). It can also mean that we *can't* regulate the internet for a host of

technological, political and national reasons. As histories of the early internet remind us, it was designed not to be controlled (Green, 2010: 24) and various attempts to block, regulate and constrain its use are, it seems, easily overcome. But more to the point, the complex issues of jurisdiction are just as much an impediment to developing any international consensus or regulatory regime. Despite the ongoing efforts of a variety of international and inter-governmental agencies, efforts to regulate or restrict the internet from the position of the nation state, it is said, lead only to greater cross-national evasion. In another sense, to say that the internet should not be regulated might also mean that there is *no need to regulate it*, or in other words that there is no problem or risk attached to it. Finally, saying no to internet regulation may also mean that for economic reasons, an unregulated and free internet best serves those commercial interests providing services on the internet as well contributing to its future development. This is largely the dominant neo-liberal discourse that has accompanied the rise of the internet and associated regulatory approaches in Great Britain, in Europe and in the wider international arena. Such an approach typically promotes models of co- or self-regulation whereby industries themselves with varying degrees of partnership or oversight by relevant state agencies practice ‘light-touch’ regulation based on codes established within the industry with minimalist prescriptions on content and with ultimate responsibility for risk exposure shifted to the end user (Freedman, 2006; Tambini, Leonardi et al., 2008).

Against this, there is increasing acceptance among policymakers that regulation in some form is in fact required to facilitate online opportunities while also reducing or managing the associated risks or downsides. Lessig has observed that at an early stage in its development utopian cheerleading for the internet gave way to the obvious realization that it contained a growing amount of increasingly dangerous material – first pornography and later deeper and more vicious threats (in Zittrain, 2008: viii). Accordingly, as he argued in *Code and Other Laws of Cyberspace* (2000), given that the internet evidently is and must be regulated, the key questions must focus therefore on regulatory choices – what, how, why and with what benefits and costs? Attempts over the past decade or so to answer these questions have generated an array of regulatory experiments, involving various forms of national and transnational governance, and new kinds of co- and self-regulatory institutional arrangements with varying degrees of accountability and effectiveness. Children’s

interests are increasingly a feature of such initiatives though the nature of those interests and how they can be best promoted remains contested.

Advocacy for child online protection

Advocacy for children's interests on the internet is sometimes presented as a polarized debate between those calling for more restrictive controls versus those wish to keep the internet free from censorship. A challenge, therefore, to the case for promoting child online protection is the oft-repeated claim that online child protection is somehow a threat to privacy and freedom of expression. The proposal to extend the Children's Online Privacy Protection Act in the U.S., for instance, was described as new battle over privacy and free speech with online safety and digital rights said to be on a collision course (Szoka and Thierer, 2009). In response to European Union proposals to extend the use of internet filtering, the claim has been made that "Free speech and freedom of communication will be the inevitable collateral damage of the building of the censorship infrastructure necessary for Internet blocking" (McNamee, 2010). In this way, child protection advocates and those promoting digital rights and freedom of expression online are typically positioned as diametrically opposed with utterly conflicting priorities in legislation, regulation and policy towards the internet.

To critics, online child protection may appear to be reactionary, overly concerned with security and a threat to the very fundamental rights of freedom of speech, free expression and participation which the internet so directly embodies. Child protection is a distinct discourse quite separate from that concerning digital rights online and it is only when they directly compete that the very different priorities and emphases emerge. As distinct and rival advocacy groups, they represent competing goals, one favouring greater regulation, control and accountability and the other supporting minimalist restrictions. But when it comes to the actual practical details about regulatory controls, the situation is more complex.

This was usefully highlighted in a forum hosted by the Oxford Internet Institute and which explored the ground between the two constituencies of child protection vs. freedom of expression (Powell, Hills et al., 2010). Participating in the debate were representatives from such contrasting organizations as the Electronic Frontier Foundation, The Progress & Freedom Foundation, and the Centre for

Democracy and Technology promoting openness, free speech rights online, and Save the Children, eNASCO (The European NGO Alliance for Child Safety Online), the National Center for Missing & Exploited Children, and ECPAT International whose focus is on promoting child protection and countering sexual exploitation online.

What was apparent from the ensuing debate is that advocates of online child protection and freedom of expression share a deep-seated belief and commitment to basic human rights even if their respective positions on regulation or measures for child protection are rarely presented in the same framework. Arguably, the interests represented by both groups are quite diverse and quite specific to the constituencies served. In practice, these opposing advocates work in quite different spheres with few opportunities to debate on common ground, and then regrettably on the basis of pitting children's interests against adult interests. Advocacy for children's interests is a broad, heterogeneous arena comprising organizations, NGOs, state agencies, individuals and policy debates seeking to protect and promote children's rights and welfare, both in the offline and online world. Many such organizations precede the internet and have long histories of providing support for child welfare issues. It is where the respective interests compete or are seen in conflict, as is the case when children's interests are pitted against the adult world, that there is need for much greater dialogue and clarification public policy goals.

On the face of it, as suggested in the forum, there is less dividing the rival perspectives than it might first appear. Freedom of expression advocates are just as committed to a safer internet and to protecting children from harm online just as child protection advocates are committed to promoting children's rights to free expression (Powell, Hills et al., 2010: 5). Common ground alone is not sufficient however to build consensus on the challenges for regulation in the interests of children. What is needed, participants to the forum agreed, is a new framework for the discussion of child protection online and that policy to be good and effective needs to be generic rather than technology-specific, use clear and precise language, and be born of real needs and targets specific risks and includes measurable goals (2010: 15).

The evidence base of risk and harm

At a policy level the opportunities and risks afforded by the internet to children and young people have attracted particular attention not least because young people tend to be in the vanguard of new media adoption, benefiting from early take-up of new opportunities afforded by the internet, mobile and broadband content, online games, peer-to-peer technologies, and so forth. Children also are also, near universally, deemed vulnerable and afforded special protection by society. In the past decade, research and policy concern has focused initially on content-related risks, particularly pornography, though aggressive, violent, gory, racist and hateful content also attracted concern. As the internet evolved from a one-to-many mass medium ('web 1.0') to a networked medium ('web 2.0'), a wider range of risks has been recognised, whether from adults or other children – notably, harassment, grooming, stalking and bullying.

The EU Kids Online network, funded under the European Commission's *Safer Internet Programme*, drawing on a database of nearly 400 studies, has classified risks encountered by children and young people first in terms of areas of the lifeworld (aggressive, sexual, values, commercial) and, secondly, in terms of the child's role (Livingstone and Haddon, 2009: 1). Therefore, risks may be deemed to consist of *content risks* in which the child is typically a recipient of potentially harmful or inappropriate content; *contact risks* where the child participates, if unwillingly, and is exposed to potentially harmful interaction with others; and *conduct risks* where the child is an actor or perpetrator of activity that may be deemed risky or potentially harmful to others – see the table below (where the cells contain exemplars only):

Table 1: Classification of types of risks facing children online

	<i>Content Receiving (typically) mass-produced content</i>	<i>Contact Participating, not necessarily willingly, in a (typically) adult-initiated activity</i>	<i>Conduct Perpetrator or victim in peer-to-peer exchange</i>
<i>Aggressive</i>	Violent / gory content	Harassment, stalking	Bullying, hostile peer activity
<i>Sexual</i>	Pornographic content	‘Grooming’, sexual abuse or exploitation	Sexual harassment, ‘sexting’
<i>Values</i>	Racist / hateful content	Ideological persuasion	Negative user-generated content
<i>Commercial</i>	Embedded marketing	Personal data abuse	Gambling, copyright infringement

Despite some cross-national variation, available findings suggest that for young people online, the experience of risks across Europe is fairly similar. Giving out personal information is the most common risky behaviour reported by about half of all teenagers; encountering pornography online is the second most common risk at about 4 in ten teenagers across Europe; seeing violent or hateful content is the third most common risk, experienced by approximately one third of teenagers; being bullied affects one in five teenagers; receiving unwanted sexual comments ranges from 1 in ten in Germany to 1 in 2 in Poland; meeting an online contact offline appears the least common though arguably the most dangerous risk and about 1 in 11 report going to such meetings. In several countries, there is evidence that around 15%-20% of online teenagers report a degree of distress or of feeling uncomfortable or threatened online. This provides some indication, arguably, of the proportion of teenagers for whom risk poses a degree of harm.

Findings from the pan-European Eurobarometer survey suggest that, according to their parents, children encounter more online risk through home than school use (though this may be because parents know little of their children’s use at school) (Eurobarometer, 2008). But since children use the internet at home for longer periods and often with less supervision, this is also likely to increase risk. Further among those (relatively few) children who use the internet in an internet café or at a friend’s house, the absence of supervision makes these risky locations.

In most countries, household inequalities in socioeconomic status have consequences for risks as well as opportunities. Specifically, even though higher status parents are more likely than those of lower status to provide their children with access to the internet, this generally enabling more use among advantaged children, it seems that lower class children are more exposed to risk online.

There are also gender differences in risk, with boys apparently more likely to encounter (or create) conduct risks and with girls more affected by content and contact risks. Specifically, boys appear more likely to seek out offensive or violent content, to access pornographic content or be sent links to pornographic websites, to meet somebody offline that they have met online and to give out personal information. Girls appear more likely to be upset by offensive, violent and pornographic material, to chat online with strangers, to receive unwanted sexual comments and to be asked for personal information though they are wary of providing it to strangers. Both boys and girls appear at risk of online bullying.

Last, it appears that older teenagers encounter more online risks than younger children, though the question of how younger children cope with online risk remains little researched.

Internet safety as a policy response

There is now wide consensus that increased access to the internet by young people across the world provides extraordinary new opportunities as well as significant negative consequences. From a policy perspective, the rapid and enthusiastic way in which three quarters of children across Europe have gone online offers a strong endorsement of the policies, infrastructural investment and initiatives undertaken to make the internet so widely accessible and available. Yet, the evidence shows that children and young people, frequently the pioneers of internet adoption, routinely encounter content that is problematic and engage in behaviour that is risky and potentially harmful. Therefore, policymakers are left with a difficult balancing act of supporting and empowering children to go online in the knowledge that increased use and higher levels of digital skills also mean increased exposure to risk (Livingstone and Helsper, 2007). The elimination of risk is neither feasible nor desirable. Therefore, efforts to minimize their occurrence focus around a greater awareness of

‘internet safety’, typically involving a multi-stranded and multi-stakeholder approach, combining legislative and regulatory interventions, awareness-raising and educational initiatives.

Internet safety policy in the European Union has evolved within an environment that has moved away from top-down, state-led models of regulation in favour of collaborative and cooperative arrangements between the state and industry. The *Safer Internet Programme*, now over ten years in existence, provides an overarching framework for European initiatives for combating illegal content, promoting safer use of internet and communication technologies and for awareness-raising activities. The Commission’s foresight in identifying issues related to risks to children in the online environment early on in the development of the internet has been widely recognised. A 1996 Communication on illegal and harmful content on the internet led to the development of two successive programmes, the Safer Internet Action Plan (1999-2004) and the Safer Internet plus programme (2005 – 2008) which established a network of Hotlines coordinated by INHOPE, the International Association of Internet Hotlines. A key achievement of the *Safer Internet Action Plan*, it is claimed, was bringing a safer internet firmly onto the political agenda of all member states, and highlighting issues of illegal and harmful content on the Internet as a serious and important political question of global dimensions (European Commission, 2008). Subsequent iterations of the programme, including the current *Safer Internet Programme (2009-2013)* have been extended to include new communication developments in mobile and broadband, web 2.0, social networking, emerging online technologies; harmful conduct such as grooming and bullying; and building the knowledge base on new trends in the use of online technologies and their consequences for children's lives.²

While to date it may be said that the priority for Europe has been a dual approach of combating illegal and criminal activity on the internet alongside efforts to foster and encourage a safer internet through better awareness and skills, there remain many dilemmas for policy makers and legislators. Maximizing internet opportunities and strongly reinforcing the Information Society agenda remains a top priority for Europe. Yet the increased hazards of the internet age and a lack of consensus on the

² See: Safer Internet Programme 2009-2013, accessed 05/09/10, http://ec.europa.eu/information_society/activities/sip/policy/program5me/current_prog/index_en.htm

scale of the problems faced make balancing empowerment a difficult task. Recently, as affirmed in the Prague Declaration (European Union, 2009), ministers of the European Union have committed to more direct coordinated, inter-governmental action to combat illegal content and to minimize risks to internet users. As a result, the European Commission has made proposals for adoption of a new directive on combating sexual abuse, sexual exploitation of children and child pornography (European Commission, 2010). At the same time, it is committed through the *Digital Agenda*, Europe's digital policy successor to i2010 (European Commission 2010), to creating a flourishing digital economy by 2020.³ This includes a set of measures to promote the building of digital confidence (p.6); guaranteeing universal broadband coverage with fast and ultra fast internet access (p.18-19); enhancing digital literacy, skills and inclusion (p.28); and promoting cultural diversity and creative content (p.30).

Internet safety and child online protection features prominently also in discussion at the Internet Governance Forum (IGF), and among other international agencies as the Internet Governance Forum, the OECD, the ITU, and the Council of Europe, as well as many national governments around the world, who all similarly engage in a tight balancing act of supporting the diffusion of new internet technologies while attempting to manage their diverse and unpredictable social consequences. The ITU, as the lead UN agency with responsibility for the internet, has been active in raising the profile of cyber security, and the role that child internet safety plays within that, not just among developed countries of the West but across the developing world where burgeoning internet adoption in Asia, Latin America and Africa greatly expands the reach of the internet and the potential risks for children. Linking internet safety with confidence and trust in the infrastructure of the internet was a theme that emerged from the World Summit on the Information Society (WSIS) in 2005 when the ITU assumed leadership of Action C5: "building confidence and security in the use of ICTs". Its Global Cybersecurity Agenda acts as the framework for international cooperation aimed at enhancing confidence and security in the information society,⁴ a central pillar of which is its Child Online Protection initiative

³ See: *Europe's Digital Agenda*, accessed 05/09/10, http://ec.europa.eu/information_society/digital-agenda/index_en.htm

⁴ See: *Global Security Agenda*, accessed 05/09/10, <http://www.itu.int/osg/csd/cybersecurity/gca/index.html>

(ITU, 2009), designed to tackle the legal, technical and institutional challenges posed by cyber security. Furthermore, building consensus and cooperation at an international level, with additional focus on issues of ICT development, requires, the ITU acknowledges, research to identify the risks and vulnerabilities to children in cyberspace, creating of awareness, sharing of knowledge and experience, and development of tools to minimize risks.

What regulation exists?

Recalling that EU Kids Online classified online risks to children in terms of content, contact and conduct risks, the regulatory approach emerging in each domain can be summarised as follows, recalling the complex mix of governance arrangements that fall under the heading of ‘regulation’, extending well beyond top-down state interventions. First, since contact risks, especially online grooming and paedophile activity, are phenomena for which society has least tolerance, these are widely though far from universally addressed by criminal law. Such legislative solutions are, however, generally reserved for high risk circumstances, since they also have the effect of constraining freedoms. The difficulty, therefore, is that they tend to presume that risk behaviours inevitably lead to harm, though in reality, children make many contacts online and only a few result in harmful encounters, albeit that these may be disastrous for their victims. Complicating matters, then, most online contacts, including most of those which lead to offline meetings, afford positive experiences for children, valuable therefore as part of their right to ‘freedom of assembly’. It is this, over and above the challenges of international law enforcement, which complicates the regulatory task of using legislative solutions to minimise contact risks to children, for it cannot easily be ascertained in advance which contacts are benign and which are harmful. Nor does research as yet pinpoint the particularly vulnerable children from among the many sufficiently resilient to avoid and/or cope with potential contact risks.

‘Content is by far the most contentious area of media policy’ (Freedman, 2008, p.122), far more than has been the case for dealing with contact risks. Difficult questions of community standards and cultural values, the basis of any filtering of content, are exacerbated in a transnational context. Yet there remains widespread

public concern that, for example, explicit images of heterosexual, homosexual, teenage, violent or bestial sexual acts are readily accessible via a simple Google search. Although traditionally tolerated in print or film, children's access to such content has traditionally been restricted, whether through regulatory or social means (Millwood Hargrave and Livingstone, 2009). Already in the short history of the internet, regulators and industry have experimented with diverse initiatives for managing the conditions of access to inappropriate content, searching for the online equivalent of these familiar (and largely uncontroversial) means of managing content offline. Yet whether implemented through white lists, black lists, walled gardens, international content rating systems, more or less subtle filters applied at different points in the distribution chain or even outright censorship, many of these initiatives have failed. Nonetheless, filters, portals or walled gardens of one kind or another remain the preferred solution on all sides, especially if installed by parents within the household, and so efforts continue to improve these (Deloitte and European Commission, 2008; Thierer, 2009). Whether or not such filters should be, by default, turned on when the computer or internet service is first purchased, by analogy with virus protection or spam filters, remains contentious, even though any adult purchaser could easily turn them off.

More recently, the risk agenda has been broadened to encompass not only how adult society may harm children but also how children's own conduct may hurt or harm each other (and even themselves). For example, bullying has long been understood as including not only physical but also verbal and visual harassment among peers (e.g. by manipulation and circulation of images). Going beyond the important point that online bullying is often continuous with offline bullying (i.e., the bully pursues his or her victim across contexts on and offline, even into their bedroom), it is increasingly acknowledged that cyberbullying differs from offline bullying insofar as it simultaneously affords anonymity to the bully and publicity to the humiliation of the victim (Smith, 2008; Vandebosch and Van Cleemput, 2009). For regulators and, indeed, the industry, conduct risks are the least amenable, for they occur peer-to-peer and are not easily (or cheaply) observed. Thus, most regulatory efforts focus on raising awareness (among parents), encouraging considerate codes of conduct (among children), facilitating peer support (via mentoring) and providing sources of support (helplines). Much effort also is directed at making young people themselves, rather than industry, self-regulating. Yet as with any effort to increase

knowledge and awareness, the reach of such initiatives is often uneven and unequal, while the translation into behaviour change is uncertain (Livingstone, 2009).

Promoting children's interests

While regulation, policy frameworks such as Europe's *Safer Internet Programme*, and the continuing policy discussions of child online protection at fora such the IGF and the ITU have made substantial contributions to a better and safer online world, internet safety remains a reactive policy response to a phenomenon that is still not entirely understood. Importantly, child online protection is a policy dedicated to reduction or elimination of cyberthreats, and strengthening action to protect children from abuse. The recognition in the WSIS outcomes that threats to children had become an online issue was an important and necessary extension to the online world of established international standards of child protection in the offline world (ITU, 2008). But it also tended to overshadow the positive dimension in the Tunis Commitment which recognized the role of ICTs in enhancing the development of children and as a means of promoting the rights of children (WSIS, 2005).

What does it mean then to promote children's interests on the internet and what are children's interests? The UN Convention on the Rights of the Child (CRC) (1989) provides the best basis for a definition and is a key milestone in giving explicit attention to children's communication rights (Hamelink, 2008). Recognizing that childhood is 'entitled to special care and assistance' (United Nations, 1989: paragraph 5), it asserts children's rights to express their views freely in all matters affecting them (Article 12); enshrines the right freedom of expression through any medium of the child's choice (Article 13); protects freedom of association and peaceful assembly (Article 15) and the right to privacy (Article 16). The CRC also specifically highlights the role of media in disseminating information that promotes the child's welfare, understood as content that promotes 'his or her social, spiritual and moral well-being and physical and mental health' (Article 17). Echoing the Children's Television Charter (World Summit on Media for Children Foundation, no date), this is further developed in (Livingstone, 2009) as a Children's Internet Charter:

- (1) 'Children should have online contents and services of high quality which are made specifically for them, and which do not exploit them. In addition to

entertaining, these should allow children to develop physically, mentally and socially to their fullest potential;

- (2) 'Children should hear, see and express themselves, their culture, their languages and their life experiences, through online contents and services which affirm their sense of self, community and place;
- (3) 'Children's online contents and services should promote an awareness and appreciation of other cultures in parallel with the child's own cultural background;
- (4) 'Children's online contents and services should be wide-ranging in genre and content, but should not include gratuitous scenes of violence and sex;
- (5) 'Children's online contents and services should be accessible when and where children are available to engage, and/or distributed via other widely accessible media or technologies;
- (6) 'Sufficient funds must be made available to make these online contents and services to the highest possible standards;
- (7) 'Governments, production, distribution and funding organizations should recognize both the importance and vulnerability of indigenous online contents and services, and take steps to support and protect it.'

An analogy may be made with the world of traditional media where the issue of children's rights has been the subject of debate for some time. The concept of 'child friendly journalism' is one that has been promoted by the Brazilian News Agency for Children's Rights - ANDI and describes a journalistic culture that not only respects, but also promotes children's rights in society.⁵ ANDI as an organization arose in the context of a society in which children's wellbeing was visibly and painfully discarded but which has also successfully achieved successful constitutional recognition in 1988 for the absolute priority of children's rights for all families, society and the state (ANDI, 2006). Through civic engagement, media partnerships, and advocacy role, ANDI uses 'social technology' to improve the

⁵ See ANDI – Brazilian News Agency for children's Rights, accessed 10 September 2010, <http://www.andi.org.br/>

quality of news media, enhance the coverage of children's issues, and to evolve a well-recognised and supported media accountability system in which the public, journalists and institutional agencies play an essential role in maintaining transparency and improving the capabilities of the media system (Jempson, 2003). It is a useful example and model for a concept of a 'child friendly internet' which similarly might be based on well-founded legislative recognition of children's rights (including communicative rights), proactive production of positive content, and an accountability system in which all stakeholders play an active role.

Conclusion

We have argued that continued and enhanced regulation is required given that large numbers of children are encountering content, contact and conduct risks on the internet, and that many children and parents may lack the tools and skills by which they can prevent or manage such exposure. While self-regulation, such as that of the mobile communications industry or by social network providers, has been a preferred approach, such industry codes in order to be effective require greater transparency and ongoing monitoring and evaluation. Inevitably, however, within the current approach to internet safety, much emphasis and responsibility falls on consumers themselves to be aware of risks and to educate themselves to be more alert to dangers on the internet (Helberger, 2008; O'Neill, 2010). eNasco, the European NGO Alliance for Child Safety Online, has called for stronger regulation in the form of unequivocal support for the EU's proposal for a directive on combating child abuse online (eNASCO, 2010). Important as this is in the creation of a safer online world, regulation remains just one factor in a complex environment constituted by technologies, different forms of social mediation, and varying levels of digital literacy, all of which require further research and greater support in developing appropriate responses to the challenge of risk and harm for young people on the internet.

References

- ANDI (2006) "Facing the challenge: children's rights and human developments in Latin American news media." from <http://www.andi.org.br/>.
- Canadian Radio-television and Telecommunications Commission (1999) Broadcasting Public Notice CRTC 1999-84.
- Commission of the European Communities (2009) Commission Recommendation on media literacy in the digital environment for a more competitive audiovisual and content industry and an inclusive knowledge society. Brussels, European Commission.
- eNASCO (2010) "The Right Click. An agenda for creating a safer and fairer online environment for every child." from <http://www.enacso.eu/>.
- Eurobarometer (2008) Towards a Safer Use of the Internet for Children in the EU: A Parents' Perspective. Luxembourg, European Commission Safer Internet Programme.
- European Commission. (2008) "Safer Internet Plus (2005-2008) Final Evaluation." from http://ec.europa.eu/information_society/activities/sip/docs/prog_evaluation/report_sip_en_2005_2008.pdf.
- European Commission (2010) Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA. Brussels.
- European Union (2009) Prague declaration A new European approach for safer Internet for children. Brussels, Council of Ministers.
- Freedman, D. (2006) "Dynamics of power in contemporary media policy-making." *Media Culture Society* 28(6): 907-923.
- Freedman, D. (2008) *The politics of media policy*. Cambridge, Polity Press.
- Green, L. (2010) *The Internet: An Introduction to New Media*. Oxford, Berg.
- Hamelink, C. J. (2008) Children's communication rights: beyond intentions. *The International Handbook of Children, Media and Culture*. H. Drotner and S. Livingstone. London, Sage: 508-519.

- Helberger, N. (2008) "From eyeball to creator – toying with audience empowerment in the Audiovisual Media Service Directive." *Entertainment Law Review* 6: 128-137.
- ITU (2008) "Press release: ITU launches initiative to protect children online." from http://www.itu.int/newsroom/press_releases/2008/33.html.
- ITU (2009) "Child Online Protection Brochure." from <http://www.itu.int/osg/csd/cybersecurity/gca/cop/brochures/index.html>.
- Jakubowicz, K. (2004) "A square peg in a round hole: The European Union's policy on public service broadcasting." *Journal of Media Practice* 4(3): 155-175.
- Jempson, M. (2003) "Children and Media - A Global Concern." from http://www.unicef.org/magic/media/documents/Children_and_media.pdf.
- Jowell, T. (2006) "Speech to the Oxford Media Convention." from <http://www.ippr.org.uk/uploadedFiles/events/Tessa%20Jowell%20Speech.doc>
- Lembke, J. (2003) *Competition for Technological Leadership: EU Policy for High Technology*. Cheltenham, Edward Elgar Publishing.
- Lessig, L. (2000) *Code : and other laws of cyberspace*. [New York, N.Y.], Basic Books.
- Livingstone, S. (2009) "A rationale for positive online content for children " *Communication Research Trends* 28(3): 12-17.
- Livingstone, S. (2010) Regulating the internet in the interests of children: Emerging British, European and international approaches. *Global Handbook of Media Policy*. R. Mansell and M. Raboy. Oxford, Blackwell.
- Livingstone, S. and L. Haddon (2009) EU Kids Online: Final report. (EC Safer Internet plus Programme Deliverable D6.5). London, EU Kids Online.
- Livingstone, S. and E. Helsper (2007) "Gradations in digital inclusion: children, young people and the digital divide." *New Media Society* 9(4): 671-696.
- McNamee, J. (2010) Internet Blocking Crimes should be punished and not hidden. Brussels, European Digital Rights.
- Nesson, C. and D. Marglin (1996) "Day the Internet Met the First Amendment: Time and the Communications Decency Act " *Harvard Journal of Law and Technology* 10(1): 113.
- O'Neill, B. (2010) "Media Literacy and Communication Rights: Ethical Individualism in the New Media Environment." *International Communication Gazette* 72(4-5): 323-338.

- Powell, A., M. Hills, et al. (2010) "Child Protection and Freedom of Expression Online." *Oxford Internet Institute Forum Discussion Paper No. 17*.
- Rheingold, H. (2000) *The virtual community: Homesteading on the electronic frontier*. Boston, MA, The MIT Press.
- Szoka, B. and A. Thierer (2009) "COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech." *Progress on Point* 16(11): 1-36.
- Tambini, D., D. Leonardi, et al. (2008) *Codifying cyberspace : communications self-regulation in the age of Internet convergence*. London, Routledge.
- United Nations (1989) "Convention on the rights of the child." from <http://www2.ohchr.org/english/law/crc.htm>.
- World Summit on Media for Children Foundation (no date) "Children's television charter." from <http://www.wsmcf.com/charters/charter.htm>.
- WSIS (2005) "Tunis Commitment." from http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|2267.
- Zittrain, J. (2008) *The future of the Internet and How to Stop It*. London, Penguin.