Sonia Livingstone
Positioning children's interests within debates over internet governance

Book section

http://eprints.lse.ac.uk

Positioning children's interests within debates over internet governance

Sonia Livingstone[1]
London School of Economics and Political Science
s.livingstone@lse.ac.uk

Introduction

As many have observed, the internet promises wonderful opportunities for learning, communicating, participating and having fun; yet the same medium is also a means of bringing into the privacy of the home the very worst of society; most online content and activities fall somewhere – often ambiguously – in between (Livingstone, 2009). Governments worldwide are not only promoting broadband infrastructure and internet use throughout society but they are also making parallel efforts to recognise and address the associated risks. The opportunities and risks afforded by the internet to children and young people have attracted particular attention, itself not always in children's best interests. Indeed, the early regulatory debates, typically led by moral panics about the internet's undermining of childhood innocence, often served to polarise rather than advance policy developments regarding online risks and opportunities.

Since those early days, regulatory debates have matured, seeking neither to establish a wholly new enterprise of online regulation but nor assuming that what holds offline straightforwardly applies online, although as a general principle this latter is accepted (van Dijk, 2006). The evidence base has also developed (as reviewed in Hasebrink, Livingstone, & Haddon; Internet Safety Technical Task Force, 2008; ITU, 2009), thereby supporting more informed multi-stakeholder deliberations. Developing the evidence base further, so as to understand which risks are encountered by which children and, crucially, when and why harm does or does not result, remains a major research task, along with the related task of identifying which policy solutions are effective – particularly, which can bring about harm reduction without also curtailing children's online opportunities. Linking these tasks is the effort to ensure that research findings are appropriately used by policy makers and other stakeholders in framing internet regulation and governance in the best interests of children.

---

[1] An earlier version of this chapter was presented at the *World Summit on Media for Children and Youth*, Karlstad (June 2010). It is based with permission on an abbreviated form of Livingstone (2011, 'Regulating the internet in the interests of children: Emerging European and international approaches', in Mansell & Raboy (Eds.), *The handbook of global media and communication policy* (Oxford: Wiley-Blackwell). It also draws material published in Livingstone, S. (2009), *Children and the Internet: Great expectations, challenging realities* (Cambridge: Polity).

This paper reflects on emerging governance practices in the United Kingdom (UK), European Union (EU) and United States (US), to explore how competing interests are being managed in practice. Specifically, I draw on my experiences in representing the EU Kids Online network in a range of policy settings, including working with the EC's Safer Internet Programme, the UK Council for Child Internet Safety and, before that, the Byron Review (Byron, 2008) and the Internet Watch Foundation in the UK. My aim is thus to combine what Bohman (1991) calls contextualised interpretation, in which the researcher draws on insider (or engaged) knowledge, and rational interpretation, in which the researcher draws on outsider (or independent, critical) knowledge. For a more developed version of these arguments, see Livingstone (2011).

Three starting points should be clarified at the outset. The first is to define children's interests, which I take from the UN Convention on the Rights of the Child (1989), also echoed in the Children's Television Charter (World Summit on Media for Children Foundation, n.d.), and set out in Livingstone (2009a: 211) 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.'

Given this deliberately ambitious conception of children's online interests, a second and complementary starting point is to identify the risks posed to children's interests by the advent of the internet. These have been classified by the EU Kids Online network first in terms of areas of the lifeworld (aggressive, sexual, values, commercial) and, secondly, in terms of the child's role. This is to distinguish content risks (which position the child as recipient), contact risks (in which the child in some way participates, if unwillingly) and conduct risks (where the child is an actor) – see the table below (where the cells contain exemplars only) (Livingstone & Haddon, 2009):

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

Balancing opportunities and risks as identified above will not happen by itself. Thus, the third crucial starting point for the present paper is to clarify what may be expected of 'governance' and 'regulation'. In this paper, I use the term regulation in the broadest sense to refer to the relation between power and the ordering of social behaviour at all levels of society from the transnational organization, the nation-state, the subnational organization or community down to the level of the individual. Without developing the point here (see Livingstone, in press), I thus position the present arguments in the context of the significant shift underway in developed market economies away from top-down, state-led models of regulation towards a conception of governance that emphasises 'the dynamic structure of rules between actors that are linked in different networks and permanently forced to negotiate, without a center that has the power to command and control' (Donges, 2007). In other words, not only has the internet brought social changes but so too is the nature of regulation and the role of the state changing; the network metaphor, intriguingly, characterises both changes (Castells, 2002).

'We will not regulate the internet'

Yet surprising to some, it is commonly claimed that – as asserted by the UK's then Secretary for State, Media, Culture and Sport, Tessa Jowell, in 2002 and echoed before and since by many others - 'we [society, the UK government] do not intend to regulate the internet'(Commons Hansard, 2002, np). If this statement was intended to forestall debate or quell contestation over internet regulation, it failed, for rapid advances in technological innovation have meant that the rationale, prospects and practicalities of internet regulation have been hotly debated throughout the past decade. So why did Jowell say this, other than for the particular, if still puzzling, reason that she was seeking to justify why the then newly-proposed regulator, the UK's Office of Communications (Ofcom), would not encompass internet regulation along with broadcasting and telecommunications regulation, despite being a converged regulator for a converged communications landscape (Livingstone and Lunt, 2007)?

Civil libertarians, clearly, hoped she – and all others who make similar claims - meant that governments *should not* regulate the internet, to protect freedom of speech and to

prevent any growth in censorship. This position holds that arguments in favour of regulation for child protection should be rejected since these threaten to restrict (adult) freedom of expression online. Thus children's needs are placed in tension with adults' needs, and in any such a balancing act of the weak versus the powerful, children will surely lose out. More subtle variants of this position fear that advocacy for child protection opens the door to censorship of speech well beyond that which may harm children and, further, to the state surveillance of citizens.

But, a simple opposition of adult freedoms and children's protection surely undermines recognition of children's positive rights, including their freedom of expression, along with adults' rights to privacy and protection from harm. Indeed, it is possible to distinguish four regulatory goals at stake – support for children's rights to freedom and to protection and support for adult's rights to freedom and to protection. Can policy makers and society agree a strategy that avoids pitting a weaker constituency against a stronger? For those following the UN Convention on the Rights of the Child (UN, 1989), the issue is that of maximizing children's online freedom while minimizing their exposure to online harm, as already noted above. Adult freedoms and rights to protection are also instantiated in national and international frameworks. The challenge is to recognise all four of these regulatory goals, not just those of child protection and adult freedom.

A second reading of Jowell's claim is that we *cannot* regulate the internet, because it is a vast and global technology, more horizontal than vertical in its structure and highly impractical to monitor. As Negroponte famously stated in 1996, '[t]he Internet cannot be regulated. It's not that laws aren't relevant, it's that the nation-state is not relevant' (cited in Drezner, 2004, p. 481). To be sure, international bodies find it difficult to attain and sustain consensus, and they typically lack the power of nation-states to enforce compliance or punish transgression. Yet this version of the claim that internet cannot be regulated tends to assume a model of top-down, command and control regulation, notwithstanding the analysis of Donges' (quoted earlier) and others regarding the growth of softer but more pervasive governance, this in turn developing partly in response to the shifting balance between national and international bodies and processes (see also Jessop, 2002). However, at least in developed countries, there are signs that international models of regulation increasingly influence rather than merely recognize or respond to the regulatory regimes of nation-states; the shifting role of regional governments such as the European Commission or the power of international organisations such as ICANN (the Internet Corporation of Assigned Names and Numbers), International Telecommunications Union or Internet Governance Forum is worth watching closely in this regard.

A third interpretation of Jowell's claim is that 'we do not intend to regulate the internet' because there is *no need* to regulate it - in short, because there is no problem. It is this argument that a wide range of child welfare professionals, children's charities, teachers and educationalists, clinicians, parenting organizations, social workers and law enforcement are marshalling their evidence to undermine, with the focus on producing empirical evidence to document the nature, incidence and severity of online harm. Nonetheless, and despite a rapidly growing evidence base regarding online risks encountered by children, the evidence remains and will remain contested, not least because the methodologies available to research children's online experiences are imperfect and because judgements of scale, reach and severity of

harm are particularly hard to ground in rigorous findings, even though these judgements are vital if policy interventions are to be proportionate. More positively, considerable efforts are now being made to generate and evaluate evidence,[2] and that which is available is no less robust than for other areas of risk for children, where regulatory protections are taken for granted (Madge & Barker, 2007).

To many critics, a fourth and final reading of Jowell's claim is the most plausible, namely that it is not that we shouldn't or can't or see no need to regulate the internet but that we *will not* regulate it, because the commercial interests at stake are substantial and, while international in scale, profits largely accrue to certain dominant nation-states. Indeed, one may even suggest that, lying behind the strongly asserted arguments that one should not regulate the internet, for reasons of free speech, or that nation states cannot hope to regulate the internet in practical terms or that the evidence base for online harm to children is flawed or inadequate, it is this argument that really drives the debate. This argument, then, treats the internet as any other business, a source of both innovation and revenue, and thus one that requires a liberalized market not hampered by 'red tape' and 'unnecessary' interference from the state. Undoubtedly, as an argument in its own right, this last is supported by many market liberals and most of the internet industry.

What is most difficult in debating internet regulation, I suggest, is not the nature of any of these four arguments but rather the persistent confusion among them, with advocates of any one position tending to shift ground and take up another position when the criticism becomes fierce, and with many arguing against internet regulation without clarifying which position they endorse or, even, the conception of regulation they are relying upon. The result can be some unholy alliances – between radical freedom of speech advocates and the industry, for example, and some unfair accusations – that to advocate child protection is to favour censorship, for example. As Szoka and Thierer (2009, p. 1) point out, in multi-stakeholder deliberations, it can too often seem that 'online privacy, child safety, free speech and anonymity are on a collision course.'

'The internet has always been regulated'

Yet, as Tambini observed, citing Lessig's (1999) ground-breaking work on *Code and other laws of cyberspac*e published well before Jowell's claim, 'of course, the internet has always been regulated' (Tambini *et al.* 2008, p. 5). To address the four arguments in turn, it should be noted first that, despite routine reference to the American constitution in defence of an anti-regulatory position, there have always been legitimate restrictions on freedom of speech, even in the US – for example, restricting the dissemination of child sexual abuse images; and such restrictions are being debated anew with the expansion of hostile, bullying and harmful speech in peer-to-peer networks among both children and adults (Collier, 2009). However, as Etzioni (2010, p. 162) observes,

> 'both individual rights and public safety must be protected. Given that on many occasions advancing one requires some curtailment of the other, the key

---

[2] See in particular the ongoing work of the EU Kids Online network at www.eukidsonline.net.

question is what the proper balance between these two cardinal values should be. The concept of balance is found in the [USA's] Fourth Amendment …'

Second, there is growing optimism that international organizations can cooperate to good effect in shaping the internet's global infrastructure - witness the increasing interest in and support for the Internet Governance Forum, notwithstanding that it has no decision-making powers, or the 2009 shift of ICANN from American to international management (ICANN, 2009). Perhaps most telling in this instance is the work of the European Commission in implementing self-regulation of mobile and social networking operators. This work and related work on privacy, personal data abuse and information rights led the European Union to endorse the ministerial Prague Declaration in April 2009, which advocates a 'holistic' cooperation across countries, including the promotion of 'a safer online environment by fostering and assessing private sector self-regulatory initiatives, and by supporting initiatives providing parental control tools as well as positive content for children' (Czech Presidency of the Council of the EU, 2009, p. 7).

Third, as evidence grows that online experiences may harm the vulnerable, including but not only children, more and more organisations (ranging from law enforcement to children's charities, schools and clinicians, businesses and governmental bodies) are extending their traditional regulatory activities from offline to online domains in order to exercise their duty of care to their clients, customers or public. In other words, it is evident to more and more bodies going about their ordinary (offline) business that the internet, far from posing no problem at all, is making a substantial difference to their operation and not always for the better.

Fourth and relatedly, there are growing calls for regulation from business as well as third sector and state actors to impose greater obligations on online service providers so as to ensure online transactions are secure, copyright infringements are enforced, personal data is well-managed and brands have their reputations protected. The ethical discourses of corporate social responsibility departments may carry little force, but the commercial interests at stake in protecting the brand carry significantly more. Consider the struggle between Facebook and its users over privacy controls (boyd & Hargittai, 2010), the effort put in by internet service providers to implement terms and conditions for customer care that meet the satisfaction of consumers, the concerted action of the industry to eradicate illegal content or to ensure that financial frauds and scams are minimised, the development of parental tools and guidance by providers keen to be perceived as 'family friendly'. All these and many other actions may be read cynically as attempts to ward off state regulation or to compete in the domestic market rather than as positive actions to advance the interest of children; nonetheless, this latter may still be the outcome.

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 & 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 & 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, Mahdavi, & Carvalho, 2008; Vandebosch & 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).

Conclusion

A recent survey of policies in place suggests considerable diversity in governance regimes worldwide, although too little is known about which forms of regulation are effective in meeting public policy goals (International Telecommunication Union, 2009). It is clear, however, that in many developed countries, regulatory regimes are generally moving towards a 'softer', more flexible, more indirect approach that disperses the role of the state, that establishes more accountable national and transnational regulatory bodies and that engages civil society (including children's welfare bodies, parenting groups and youth organisations) in processes of governance. In parallel, considerable efforts are being made to devolve regulation down to the level of the individual, encouraging in individuals (parents, teachers, children) the responsibility to conduct their own personal risk assessment. As Beck (1986/2005) put it, in the 'risk society', risk has been individualised. Consequently, everyone 'need[s] to adopt a calculative prudent personal relation to fate now conceived in terms of calculable dangers and avertable risks' (Rose, 1996, p. 58).

But Beck and Rose are critical of a situation popularly described as 'empowering' for the individual. First, it tasks individuals with sometimes burdensome responsibilities for which they may lack resources or for which resources are unequally distributed. Second, the dispersal of regulation from state to self-regulation means that governance approaches "commonly lack[s] the procedural fairness and protection for fundamental rights that are encouraged by independent judicial and parliamentary scrutiny" (Brown, 2010; see also Schultz & Held, 2006). To equip individuals, governance regimes place increasing reliance on media or digital literacy policies, as in, for instance, the EU's Digital Agenda (European Commission, 2010; for the rising importance of media literacy as a tool of regulation, see Livingstone, 2009). To introduce principles of fairness, transparency and accountability into self-regulation, governance regimes often include some degree of oversight – where 'oversight' refers to 'second-order processes' which 'examine, review, and correct first-order processes'; this, Etzioni (2010, p.175) argues is the second crucial balance to be achieved in regulation – 'not between the public interest and rights, but between the supervised and the supervisors' (p.174).

Recent examples include the EC Safer Internet Programme's independent evaluation of filtering technology (Deloitte and European Commission, 2008), of the Mobile Operators' Code (PricewaterhouseCoopers, 2009) and, most recently, of the Social Networking Guidance (European Commission, 2009). In relation to both sets of policies – those addressing individuals' competence and those addressing firms' responsibilities – consideration for children's risks and opportunities online has led the way; nonetheless, the resulting governance approaches are couched in more general terms, benefiting (or otherwise) the wider public. Intriguingly, there is a degree of complementarity between media literacy policy (which is necessarily

limited by the bounds of individuals' competence) and industry self-regulation (which is expected to step in as required to support the needs of individuals). For example, if children and parents understand and respect the rule that those under 13 years old are not permitted on Facebook or MySpace, then the social networking site need take no action; but insofar as individuals do not understand or respect this rule, the site is expected to take action as part of its self-regulatory guidance. Similarly, to the extent that parents lack the skill to install filtering technology, then technology providers are expected to redesign their products and provide a help desk. And so forth. In other words, the affordances of the online interface can be designed to fit more or less well with the literacies of users, and the result is more or less enabling or undermining of use.

In cases where the risk at stake is unambiguous or uncontroversial, most would agree that the online environment should be designed so that little or no reliance is placed on the individual's competence: examples might include preventing paedophiles from using social networking sites popular with children or ensuring that financial fraud is eliminated by securing payment systems; to rely on the competence of children in such cases seems unnecessarily hazardous. In such cases, a strategy of 'safety by design' (as already occurs in offline in the domains of engineering, urban planning, health and safety at work) can reduce risk without affecting opportunities. But in cases where the risk at stake is ambiguous (for example, making new online contacts may be beneficial but may be dangerous) or controversial (for example, is seeing online pornography harmless or harmful?) or dependent on circumstances (for example, most children are not tempted to take the advice of pro-harm sites but a few are vulnerable to such advice), the online environment cannot simply be designed to be risk free, for this is to undermine individual opportunities. Even then, 'safety by design' can reasonably be employed to reduce risks provided that individuals' choices are not prevented entirely: examples might include the use of default filters that can, if desired, be overridden, or programmed-in reminders on sending images or posting personal information to think carefully before acting. Though the effect of such features is likely to increase media literacy, this remains to be established by empirical research.

As should be apparent, in this paper I have sought to move beyond a framework for children's interests that simply polarises consideration of online risks and opportunities, also rejecting a framework for regulation that simply polarises top-down restrictive regulation and laissez-faire avoidance of regulation in the interests of (adult) freedoms. The task for researchers, therefore, is no longer primarily to chart the possible harms experienced by children online, in order to provoke regulatory intervention. Rather, a more complex research agenda is opened up, matching the complexity of the emerging governance regime as well as the complexity of children's interests online. In short, researchers should investigate (and many now are investigating) the conditions of childhood that mean some children explore online opportunities and become resilient to the risks while (a few) others get hurt. However, they should also investigate (and here much more research is needed) the conditions of the online environment that render some sites more or less beneficial or hazardous, as a function of their design and institutional infrastructure as well as their practices of use, and some regulatory tools and strategies more or less effective, depending in part on their implications for media literacy.

References

Beck, U. (1986/2005). *Risk society: Towards a new modernity*. London: Sage Publications.

Bohman, J. (1991). *New philosophy of social science: Problems of indeterminacy*. Cambridge: Polity Press.

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday, 15*(8).

Brown, I. (2010). Internet self-regulation and fundamental rights. *Index on Censorship, 1*, 98-106.

Byron, T. (2008). *Safer children in a digital world: The report of the Byron Review*. London: Department for Children, Schools and Families, and the Department for Culture, Media and Sport.

Castells, M. (2002). *The Internet galaxy*. Oxford: Oxford University Press.

Collier, A. (2009). School cyberbully wins free-speech case. *Journal*. Retrieved from http://www.netfamilynews.org/2009/12/school-cyberbully-wins-free-speech-case.html

Commons Hansard (2002). "House of Commons Hansard Debates for 3 Dec 2002 (pt 14)", accessed 01/01/2010, http://www.parliament.the-stationery-office.co.uk/pa/cm200203/cmhansrd/vo021203/debtext/21203-14.htm

Czech Presidency of the Council of the EU (2009). "Prague declaration: A new European approach for safer Internet for children" (20 April), Prague: Ministerial Conference 'Safer Internet for Children – fighting together against illegal content and conduct on-line', accessed 03/01/2010, http://ec.europa.eu/information_society/activities/sip/docs/events/prague_decl.pdf.

Deloitte, and European Commission (2008). *Safer Internet: Protecting our children on the net using content filtering and parental control techniques: A report prepared for the Safer Internet Plus Programme*. Belgium: Deloitte Enterprise Risk Services, accessed 03/01/2010, http://www.sip-bench.eu/index.html .

Donges, P. (2007). The new institutionalism as a theoretical foundation of media governance. *Communications: The European Journal of Communication Research, 32*(3), 325-329.

Drezner, D. W. (2004). The global governance of the Internet: Bringing the State back in. *Political Science Quarterly*, 119(3), 477-498.

Etzioni, A. (2010). Privacy and security policy in the digital age. In W. R. Newman (Eds.), *Media, technology, and society*. Ann Arbour: University of Michigan Press (pp. 163-178).

European Commission (2009). "Safer social networking principles for the EU", Brussels: European Commission, accessed 03/01/2010, http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

European Commission. (2010). *A digital agenda for Europe*. Brussels: European Commission.

Freedman, D. (2008). *The politics of media policy*. Cambridge: Polity Press.

Hasebrink, U., Livingstone, S., & Haddon, L. (2009). *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online*. Deliverable D3.2 for the EC Safer Internet plus programme (Second edition). London: EU Kids Online, accessed 01/01/2010, http://eprints.lse.ac.uk/24368/ .

ICANN (2009). *Affirmation of commitments by the United States Department of Commerce and the Internet corporation for assigned names and numbers*. Washington, DC: Internet Corporation for Assigned Names and Numbers, accessed 03/01/2010, http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm .

International Telecommunication Union (2009). *Child online protection*. Geneva: International Telecommunication Union, accessed 03/01/2010, http://www.itu.int/osg/csd/cybersecurity/gca/cop/cop-brochure.pdf .

Internet Safety Technical Task Force. (2008). *Enhancing Child Safety and Online Technologies: Final Report of the ISTTF to the Multi-State Working Group on Social Networking of State Attorney Generals of the United States.* Cambridge, MA: Berkman Center for Internet and Society, Harvard University.

Jessop, B. (2002). *The future of the capitalist state*. Cambridge: Polity Press.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Livingstone, S. (2009). *Children and the Internet: Great expectations, challenging realities*. Cambridge: Polity Press.

Livingstone, S. (2009a). A rational for positive online content for children. *Communication Research Trends*, 28 (3), 12-17.

Livingstone (2011), '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).

Livingstone, S., & Lunt, P. (2007). Representing citizens and consumers in media and communications regulation. *The Annals of the American Academy of Political and Social Science, 611*, 51-65.

Livingstone, S., & Haddon, L. (2009). *EU kids online: Final report*. Deliverable D6.5 for the EC Safer Internet plus programme. London: EU Kids Online, accessed 01/01/2010, http://eprints.lse.ac.uk/24372/ .

Madge, N., & Barker, J. (2007). *Risk & childhood*. London: The Royal Society for the Encouragement of Arts, Manufactures & Commerce.

Millwood Hargrave, A., & Livingstone, S. (2009). *Harm and offence in media content: A review of the empirical literature* (Second edition). Bristol: Intellect Press.

PricewaterhouseCoopers (2009). *European framework for safer mobile use by younger teenagers and children*. London: PricewaterhouseCoopers, accessed 01/01/2010, http://www.gsmeurope.org/documents/PwC_Implementation_Report.pdf.

Rose, N. (1996). Governing 'advanced' liberal democracies. In A. Barry, T. Osborne & N. Rose (Eds.), *Foucault and political reason: Liberalism, neo-liberalism and rationalities of government* (pp. 37-64). London: UCL Press.

Schulz, W., & Held, T. (2006). Together they are strong? Co-regulatory approaches for the protection of minors within the European Union. In U. Carlsson (Ed.), *Regulation, awareness, empowerment: Young people and harmful media content in the digital age* (pp. 49-65). Göteborg: Nordicom.

Smith, P. K., Mahdavi, J., & Carvalho, M. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49*(4), 376-385.

Szoka, B., & Thierer, A. (2009). COPPA 2.0: The new battle over privacy, age verification, online safety & free speech, *Progress on Point, 16*(11), accessed 03/01/2010, http://pff.org/issues-pubs/pops/2009/pop16.11-COPPA-and-age-

verification.pdf.

Tambini, D., Leonardi, D., & Marsden, C. (2008). *Codifying cyberspace: Communications self-regulation in the age of Internet convergence*. London: Routledge.

Thierer, A. (2009). *Parental controls & online child protection: A survey of tools and methods*. Washington, DC: The Progress & Freedom Foundation.

United Nations (1989). *Convention on the rights of the child*, accessed 29/1/2008, http://www2.ohchr.org/english/law/crc.htm.

Van Dijk, J. A. G. M. (2006). "Law", in J. A. G. M. Van Dijk (Ed.), *The network society: Social aspects of new media* (pp. 127-155). London: Sage Publications.

Vandebosch, H., & Cleemput, K. V. (2009). Cyberbullying among youngsters: profiles of bullies and victims. *New Media & Society, 11*(8), 1349-1371.

World Summit on Media for Children Foundation. (n.d.). Children's television charter, accessed 05/8/2010, http://www.wsmcf.com/charters/charter.htm