Regulating the internet in the interests of children: emerging European and international approaches

Book section

Original citation:
Livingstone, S. (2011) Regulating the internet in the interests of children: Emerging European and international approaches. In Mansell, R., and Raboy, M. (Eds.) The Handbook on Global Media and Communication Policy (505-524). Oxford: Blackwell.

Regulating the internet in the interests of children: Emerging European and international approaches

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

Introduction

> 'Online privacy, child safety, free speech and anonymity are on a collision course' (Szoka and Thierer 2009: 1).

Governments around the world are actively promoting internet infrastructure, diffusion and use in the workplace, schools, communities and households. There is growing consensus that if this is to serve the interests of the public, including – my concern here - children and young people, policy-makers must determine how best to facilitate online opportunities while also reducing or managing the associated risks. Although there remain difficulties in identifying just what opportunities and risks the internet might afford, many initiatives are underway nationally and internationally to establish a regulatory regime for the online environment, partially though not wholly paralleling the regulation of the offline environment. Drawing mainly on an account of emerging governance practices in the United Kingdom (UK) and Europe, though noting the strong influence on these of United States (US) industry, regulator and child welfare advocacy, I ask how competing interests can be, and are being managed in practice. My aim is to capture recent debates and practice regarding the protection and empowerment of children online, although my broader rationale in favor of (careful and proportionate) regulation may apply to other 'vulnerable' or minority groups or even to the protection and empowerment of the public at large.

I begin, not with matters of regulation but with children's experiences of the internet. There is increasing evidence that the internet amplifies and intensifies the nature of childhood (and adult) experiences. On the one hand, children's avenues for participation, their resources for education and their circles of connection for friendship and intimacy are all expanded and more accessible (boyd 2008; Dahlgren and Olsson 2008; Ito *et al.* 2008; Willett 2008). It is evident that, given minimal conditions of access and literacy, children relish the opportunities afforded by the internet, often responding to these in creative, diverse and highly literate ways. However, empirical analysis of children's online experiences qualifies the popular rhetoric regarding 'digital natives' (Bennett, Maton and Kervin 2008), suggesting that society must be realistic about their skills and look beyond children's enthusiasm when formulating policies to ensure fairness of opportunity, ambitious expectations

for participation and digital literacies and, not least, reasonable expectations of safety for all (Livingstone 2009).

At the same time, evidence is also growing that the internet amplifies and intensifies the risk of harm to children (Muir 2005). For a child victim, an image of abuse may now be distributed anywhere worldwide in a matter of seconds and never eradicated (Internet Watch Foundation, IWF 2008). For the bullied child, a hostile site morphing their image or inviting ridicule may harm them anywhere, anytime, hostility even reaching into their bedroom (Nightingale, Dickenson and Griff 2000). For a teenager in despair, a community of suicidal others advocating the means of self-harm may be reached at the click of a mouse with a convenience that is historically unprecedented (Alao, Soderberg, Pohl and Alao 2006). And for the young bully or racist, the internet affords new and convenient means of harming others that are not easily detectable (Barak 2005; Shariff and Churchill 2010). It is not that online risks are necessarily unfamiliar in and of themselves. Rather, the ways and possibly the extent to which children now encounter these familiar risks is distinctively new – faster, more privatized and more permanent, with the most inclusive access to tools for image production and distribution ever known, thereby enabling both extensive circles of influence and many unanticipated consequences.

Children's everyday contexts of internet use combine experiences of both opportunities and risks, forcing the belated recognition that these often go hand in hand, the former tending to increase rather than decrease the chances of encountering the latter. This poses difficult questions of balance in managing children's online experiences, for policy relating to opportunities must be integrated with, rather than remain entirely separate from that relating to risk and safety (Livingstone 2009). Celebrating young people's enterprise and enthusiasm while failing to engage with or support their online activities or their experience of online harms will surely fail to bring to fruition the great expectations society holds not only for the internet but also for children. How far, then, should policy-makers facilitate the provision of resources – to promote such positive goals as online education, participation, creativity and so forth?[2] How far can the (young) people's digital literacy be relied upon for judicious navigation of the internet or is regulation required to ensure sufficient protection (Livingstone 2008)? Are online risks best addressed by particular agencies, and at international, national or community levels?

Although we still lack robust answers to these questions, the emerging consensus is that maximizing opportunities while minimizing risks is a task for multiple stakeholders, requiring not only financial investment but also adaptation to rapid change, apportioning responsibility flexibly among relevant parties, applying local or national experience to confront a global phenomenon and learning new forms of expertise. But is this the optimal approach, and how is it working in practice?

Positive and Negative Internet Regulation in the Interests of Children

Early in the internet's history, two problematic claims were much reiterated: first, that the internet should not be regulated at all and second, that even arguments that regulation would protect children must be rejected since these may have the consequence, deliberate or otherwise, of restricting (adult) freedom of expression online. Echoes of both claims persist in current multi-stakeholder dialogues,

especially when matters become fraught. Although few would make such bald assertions today, their legacy is discernable in the tendency of policy discourses to pit child protection against adult freedom of expression. Most simply, this results in a rhetoric which puts children's needs in conflict with those of adults; and in such a balancing act of the weak versus the powerful, children will surely lose out. Even in more complex debates, there is frustration when protectionist voices from child and family welfare constituencies seem to legitimize a brake on either personal or commercial freedoms. Consider Castells' (2002: 169-70) comment on the overturning of the 1996 Communications Decency Act:

> 'Control of information has been the essence of state power throughout history… This is why one of the exemplary values of the American Constitution is precisely to place the right to free speech as the First Amendment of the Constitution. In their attempt to exercise control over the Internet, the US Congress and the US Justice Department used the argument that strikes a chord in every one of us: the protection of children from the sexual evils roaming the Internet'.

Or, as Raboy and Shtern (2010: 219) observe more recently, '[a]t the 2008 IGF [Internet Governance Forum] for example, the push for online child protection was perceived to be a threat to privacy and freedom of expression rights'.[3] Policy efforts may even seem to minimize attention to children's interests in order to promote adult freedoms. However, as I note below, the early arguments against internet regulation have been strongly rebutted first by legal theory regarding cyberspace and second, by advocates of children's rights online as well as offline. As Lessig (1999) observes, since the internet is and must be regulated, the key questions focus 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 nationally and internationally.

There is a further reason why any simple opposition of adult freedom and child protection must be transcended, and that is that it undermines recognition of both children's positive rights (including freedom of expression) and adults' rights to privacy and protection of harm. Indeed, one may identify four distinct regulatory goals at issue here – support for children's rights to freedom and to protection, and support for adult's rights to freedom and to protection. In calling for a balanced approach to regulating the internet in the interests of children, therefore, I hope to avoid pitting a weaker constituency against a stronger by reframing the regulatory challenge for each constituency separately. Thus, I focus primarily on the task of maximizing children's online freedoms while minimizing their exposure to online risks (a balance required also by the 1989 United Nations (UN) Convention on the Rights of the Child; Hamelink 2008). Some of the arguments that follow have wider implications for the parallel balance to be achieved between adult freedoms and adult protection (witness recent concerns about privacy, data protection, copyright infringement, bullying, spam, phishing and other scams, etc.).

It should be noted that I use the term 'regulation' in the broadest sense, referring to the relation between power and the ordering of social behavior, at any and all levels of society from the transnational organization, the nation-state, the subnational organization or community and/or the individual. I then follow the contemporary

theorists of the state (see Jessop 2002) who argue that Western advanced industrial democracies are undergoing a profound shift in regulatory regimes from a government-led 'command-and control' model to a mixed model of *governance* encompassing state, co- and self-regulation, thereby dispersing power away from the state, often to newly powerful transnational bodies. For academic and policy observers, this shift raises significant questions about the legitimacy, authority, accountability and effectiveness of different forms of regulation, as well as about the increasing complexity of their interrelations. But before addressing today's complex situation, let us consider a simple and, at the time, popularly endorsed claim, below.

'We do not intend to regulate the internet'

In 2002, the UK's then Secretary for State, Media, Culture and Sport, Tessa Jowell, announced, 'we do not intend to regulate the internet' (Commons Hansard 2002: np). Accordingly, the 2003 Communications Act established Ofcom, the UK's new, converged regulator for a newly convergent media environment, with no requirements regarding the internet in its remit. Nonetheless, spurred on by rapid advances in technological innovation combined with an unstable economy, the possible rationale for internet regulation has been much debated during the last decade, in the UK and elsewhere (Tambini *et al.* 2008). Particularly, multiple justifications for internet regulation have, increasingly if sometimes reluctantly, become widely accepted following the publication (notably pre-dating Jowell's speech) of Lessig's (1999) *Code and Other Laws of Cyberspace*. Some reflect a concern for the interests of children or other vulnerable or minority groups, though they also reflect the concerns of the private sector (especially in relation to market freedoms, intellectual property and copyright) and the state (especially in relation to privacy, data protection and threats to national security). Undoubtedly, internet regulation is fast rising up the policy agenda. For example, the UK's All Party Parliamentary Communications Group released a report in October 2009 entitled 'Can we keep our hands off the Net?'[4] which gathered together many and diverse calls for regulation, echoing those on the agenda of the fourth annual meeting of the UN Internet Governance Forum held in Egypt in November 2009.

So, what did the Secretary of State mean when she declared that 'we do not intend to regulate the internet'? Many libertarians hoped this meant we *should not* regulate the internet for reasons of freedom of speech and against any policies of censorship. Concern over the slippery slope argument – that advocacy for the protection of children opens the door to censorship of content for adults and even the state surveillance of citizens – has been expressed by many critics (Brown 2008; Petley 2009), especially those concerned with the US's First Amendment and the legitimacy of any qualifications to this (for example, the 'right' to hostile or hate speech in the US in schools is not protected, raising interesting questions regarding the regulation of cyberbullying).[5] A well known illustration of this clash of interests was the successful attack (in defence of civil liberties) by the Electronic Frontier Foundation on the US's Communications Decency Act, 1996 (designed, among other things, to prevent online pornography reaching children; Murray 2007).

A second reading of Jowell's claim is that we *can't* regulate the internet – because it is a vast and global technology, horizontal more than vertical in its management structures, and as impractical to monitor (as for postal and telecommunications

services) – hence the early provision of mere conduit[6] restrictions on internet service provider liability (Brown in press). 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: 481). The internet, it is held, evades the jurisdiction of any one government, and attempts to impose regulatory restrictions will not only be undermined by network architecture but also suffer the unintended consequence of encouraging evasion and subterfuge of ever more ingenious kinds (Murray 2007; Tambini *et al.* 2008). Moreover, international bodies find it near-impossible to sustain consensus, and they lack the power of nation-states to enforce compliance or punish transgression.

Two further readings are also possible. One 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 here that the range of child welfare professionals – children's charities, teachers and educationalists, clinicians, parenting organizations, social workers and law enforcement - have focused their arguments, marshalling evidence to scope the nature, incidence and severity of online harm. A series of comprehensive evidence reviews undermine any claim that the internet poses no risk to children (Muir 2005; O'Connell and Bryce 2006; Byron 2008; Internet Safety Technical Task Force 2008). Having reviewed the evidence available in Europe, the EU (European Union) Kids Online network, which I direct for the European Commission (EC) Safer Internet Programme, classified online risks (and opportunities) so as to clarify future directions for public policy interventions and, especially, to transcend the over-simple rhetoric of both child-as-victim and child-as-digital-native (or indeed, child-as-villain).

First, we distinguished content risks in which the child encounters unwelcome or inappropriate content, from contact risks in which the child becomes a participant in risky personal communication (Hasebrink, Livingstone and Haddon 2009). Content risks arise because little regulation restricts the distribution of harmful websites (compare with the commonplace regulation of television, film and print). Thus children encounter more diverse and extreme content online than from other/older media. Surveys in Europe suggest one in four teenagers have encountered online pornography (though little is known of the nature of this material) and one in three have encountered online hate or violent content (Livingstone and Haddon 2009). Contact risks arise because little regulation restricts who can be in touch with anyone else online, and they are exacerbated by the ease with which age can be disguised online and the difficulty of ensuring privacy for personal information. While evidence is growing that risky contacts may expose children to harmful online experiences (e.g., sexual harassment through ab/use of webcams; National Campaign to Support Teen and Unplanned Pregnancy 2008),[7] public concern focuses on the likelihood that online communication with new contacts (whether labelled 'strangers' or 'friends') results in abusive meetings offline. EU Kids Online found that one in ten European teenagers has gone to a meeting with a contact s/he first met online, though very few of these result in harm. Some British (Child Exploitation and Online Protection Centre, CEOP 2009) and American (Wolak, Finkelhor, Mitchell and Ybarra 2008) research suggests that the incidence of online grooming resulting in offline crimes against minors is rising.[8]

With the explosion of user-generated content, some hosted on professional, commercial websites (e.g., social networking, gaming or blogging sites) and some circulated peer-to-peer (e.g., via email, instant messaging or newsgroups), the distinction between content and contact is blurring. Thus a third category of risk is proposed, that of conduct among peers: to understand these risks we must position the child as an actor who contributes to online risk, deliberately or unwittingly, as part of his or her peer-to-peer engagement. Attention has especially focused here on cyberbullying (Smith, Mahdavi, Carvalho and Tippett 2006; Shariff and Churchill 2010), estimated by EU Kids Online to affect one in five teenagers (as victims, and fewer as perpetrators although – challenging for policy-makers – both roles may be taken by the same child; Wolak *et al.* 2008).

Despite a fast-growing evidence base regarding online risk to children, the evidence remains contested and the methodologies available are imperfect, this impeding the judgements of scale, reach and severity necessary if policy is to be proportionate in balancing competing demands (Lobe, Livingstone and Haddon 2007). Nonetheless, the evidence is no less robust than for many other areas of risk for children (Madge and Barker 2007), where regulatory protections are taken for granted. Recently, the evidence for content, contact and conduct risks to children on the internet led the European Union to endorse the ministerial Prague Declaration in April 2009, setting out 'a new European approach for a safer internet for children'. This 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: 7). A range of existing and new policy initiatives are thereby brought together, albeit mainly reliant on the cooperation of individual Member States and/or European-level self-regulatory activities (notably, as coordinated by the Directorate-General Information Society's *Safer Internet Programme*; see Reid 2009).

Of course, it is the fourth reading that is most plausible - 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. In 2005, Jowell (Department for Culture, Media and Sport 2005: np) gave a speech to the industry that exemplified this reading:

> 'We don't want to use a sledge-hammer to crack a nut … Creativity and enterprise can't flourish if they are beset by reams of red tape. … Regulation has to be proportionate, and take into account the opinions and needs of the businesses it is trying to regulate….And we should also remember that the international community can only do so much'.

So, while the first reading treats the internet as a particular case of speech, the second treats it as too elusive for national regulation and the third as offering only a dubious case for intervention, this fourth argument treats the internet as any other business, a source of both innovation and revenue that demands a liberalized market not to be hampered by 'red tape'. Just as the British government resisted the more restrictive proposals of the Audiovisual Media Services Directive (so as to liberalize communication markets), in relation to the internet too, Britain and America appear to

lead the Western argument against regulation. On the other hand, the recent establishment of a UK Council for Child Internet Safety reveals British Government support for compensatory efforts towards concerted and effective self-regulation. The Family Online Safety Institute, a multi-stakeholder alliance of mainly industry players, primarily but not only based in the US, is seeking similar support. Also noteworthy of coming changes are the Department of Commerce's Online Safety and Technical Working Group, whose subcommittees on pornography, data retention, parental controls and consumer online safety education are due to report in June 2010,[9] and the Federal Communications Commission's notice of inquiry issued in October 2009 on 'empowering parents and protecting children in an evolving media landscape' (Federal Communications Commission 2009: np).

'Of course, the internet has always been regulated' (Tambini *et al.* 2008: 5), in recognition of the limitations of the above readings (see Lessig 1999). First, there have always been legitimate restrictions on freedom of speech (even in the US – for example, the dissemination of child sexual abuse images), these attracting more attention with the expansion in hostile and harmful speech in peer-to-peer networks. 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, or the 2009 shift of the Internet Corporation for Assigned Names and Numbers (ICANN) from American to international management; see chapter by Klein in this volume). Third, there is growing evidence that online experiences may harm the vulnerable, including but not only children, this requiring greater care over the interests of ordinary users. Fourth, 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.

Children's Rights Offline and Online

> 'The child/media relationship is an entry point into the wide and multifaceted world of children and their rights – to education, freedom of expression, play, identity, health, dignity and self-respect, protection … in every aspect of child rights, in every element of the life of a child, the relationship between children and the media plays a role' (United Nations Children's Fund, UNICEF 1999: np).

Principled arguments against regulatory interference in relation to either or both of the global market and adult freedom of speech have been met with equally principled arguments in support of children's rights, concerning both their rights online and the implications of the internet for their rights offline. The UN Convention on the Rights of the Child (United Nations 1989), ratified by all countries but Somalia and the US, asserts the rights of all those under eighteen years old across all dimensions of children's lives, including both positive (enabling) and negative (protective) communication-related rights (Hamelink 2008). Ten years on, UNICEF (1999) asserted the specific relevance of this rights agenda to the media in its 'Oslo Challenge' above. In a digital age, these rights – of freedom of expression and association, to beneficial material in one's own language, to privacy and to protection from harmful material – undoubtedly extend online as well as offline.[10] One way

forward would be to establish a Children's Internet Charter (Livingstone 2009a) to mirror the earlier Children's Television Charter. Relatedly, in 2007 the Council of Europe advocated, as an extension of the notion of public service from broadcasting to the internet: [11]

> 'The concept of public service value of the Internet, understood as people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions) and the resulting legitimate expectation that Internet services are accessible and affordable, secure, reliable and ongoing' (Council of Europe 2007: np).
> Tangible initiatives in support of media or digital literacies (Livingstone 2008;

Frau-Meigs and Torrent 2009) also advance positive communication rights online, as would increased provision resulting from the EC Safer Internet Programme's call for more 'positive content' online (European Commission 2009).[12] Without being po-faced about what's good for children, and noting that children may disagree with adults when evaluating online opportunities, it is both important and timely to call for content, contact and conduct that benefits children – whether this is specifically online public service content (i.e., provided by a public service institution and evaluated for being diverse, indigenous, high quality and stimulating) or the more mixed provision of opportunities for content, contact and conduct that enable children's online interaction and communication. How children's digital rights and opportunities may be implemented remains unclear, though an audit of what is available to and accessible by children in different countries and life contexts would be a useful step.

An important feature of the Convention on the Rights of the Child is that it brings together children's positive and negative rights. Empirically, as noted earlier, opportunities and risks tend to be positively associated, although it also seems that the more children are provided with 'positive content' the less they surf randomly and so encounter online risks (Bauwens *et al.* 2009).[13] Theoretically, the linking of opportunities and risks is central to what Beck has termed 'the risk society'(1986/2005). On the internet, this linkage is particularly difficult to manage. Not only do children engage in both 'approved' and 'disapproved' activities, but often these are the same activities – to take up an opportunity, one may encounter a risk; as in the offline world, 'twas ever thus. This may be exacerbated or ameliorated by the environment in which children grow up: both urban and online environments are largely designed for and populated by adults - their affordances are never neutral and rarely child-friendly (after all, the early founders of the internet arguably never imagined that children would become users, and in substantial numbers). On an individual level, the close relation between opportunities and risks is significant, for as child psychologists observe, children learn by extending themselves, stretching their capacities and encountering both the unexpectedly beneficial and the problematic in order to gain resilience (Vygotsky1934/1986). The more children are to learn online, the more they must gain resilience in managing the online environment.

Internet Regulation – Emerging Principles and Practices

> ‘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: np).

Especially but not only in Western advanced industrial democracies, the widely favored solution to the challenges of internet regulation is self-regulation, this requiring cooperation across a heterogeneous array of hardware, software and content providers, largely from the private sector but including significant public sector elements. This is consistent with the wider shift in regulatory regimes from (direct or top-down) government to dispersed and often indirect governance characteristic of neoliberalism (Freedman 2008). As Donges (2007: 326) observes,

> ‘governance refers to 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’.

While such a dynamic process of regulation has some advantages, as noted below, it does make for piecemeal policy-making across a heterogeneous array of organizations and alliances.[14] In the case of internet regulation, this renders it hard to assess whether, as critical accounts of the struggles between industry and educators/third sector would question, self-regulation is serving the long-term interests of children as much as it does those of the private sector.

Usefully, self-regulation avoids the problematic ‘we’ that so easily undermines the rationale for internet regulation – for who are ‘we’ to decide to restrict online activities, especially when the ‘we’ who decides may not equate to the ‘we’ in whose interests such decisions are made? In an age when public trust seems to elude governments, it seems expedient to pass the regulatory task to the internet industry itself, with slippery matters of offence, values and conduct to be managed through company policy, customer care relations and/or technological means. The ‘we’ who regulates therefore, is the industry acting, as it may be trusted so to do, out of self-interest (to protect the integrity of its service, the confidence of its customer base and the reputation of its brand) rather than in the public (or children’s) interest, though such interests need not be incompatible.

Provided such self-regulation is effective or, failing that, transparent in its efforts (i.e., provided the customer can detect and evaluate the regulatory tools and procedures implemented by the provider), then ‘we’ the public are (supposedly) free to choose the services that best support our desired balance of opportunities and risks. But if the effectiveness and/or transparency of self-regulation are not established, regulatory alternatives could and, arguably, should be sought. Scott (2001: 3) defines the relation between regulation and social control as encompassing:

> ‘(1) some sort of standard, goal, or set of values against which perceptions of what is happening within the environment to be controlled are compared through (2) some mechanism of monitoring or feedback which in turn triggers (3) some form of action which attempts to align the controlled variables, as they are perceived by the monitoring component with the goal component’.

Traditionally, these goals are set by the state, to advance the interests of public or market or both, while monitoring and compliance roles have been undertaken by a command-and-control style regulator. Hence:

> 'For classical regulation the goal component is represented typically by some legal rule or standard, the feedback component by monitoring by a regulatory agency, government department or self-regulatory organisation and the realignment component by the application of sanctions for breach of standards' (Scott 2001: 3).

As consensus grows that top-down supervisory regulation (usually by governments or their appointed agents) is no longer optimal, especially in the fast-globalizing media and communication sector, the jury is out over the relative merits of co- and self-regulation, the two main alternatives. While the US favors a mix of legislation and self-regulation (Montgomery 2007) and Europe favors co-regulation (or what Christou and Simpson (2006) term 'public-private transnational governance'), the UK prefers a strategy of self-regulation (Tambini *et al.* 2008). Held (2007: 357) defines co-regulation in terms of the following criteria, emphasizing the vital role of the state in ensuring the legitimacy and effectiveness of regulatory bodies:

> '(1) The system is established to achieve public policy goals targeted at social processes. (2) There is a legal connection between the non-state regulatory system and the state regulation. (3) The state leaves discretionary power to a non-state regulatory system. (4) The state uses regulatory resources to influence the outcome of the regulatory process (to guarantee the fulfilment of the regulatory goals)'.

By implication, self-regulation occurs when only the first and third criteria are in place. The second and fourth criteria afford pressure points for the state, in addition to the threat (often discursively salient in today's governance regimes) that legislation will be introduced should self- or co-regulation prove insufficient to achieve desired public policy goals. But even the first and third points are not straightforward: who is to set the goals for self-regulation and how it is to be managed and evaluated remain the subject of both explicit and behind-the-scenes contestation. This is unsurprising given conflicting interests across public and private sectors and given that cooperation is required across national and international levels of organization.

Since self-regulation offers a means of dispersing power from the centralized state to a host of institutions with governance responsibilities at all levels from local to global (Jessop 2002), one crucial consequence is that 'it is increasingly difficult to uphold a clear distinction between *public* and *private* governance arrangements' (Zürn and Koenig-Archibugi 2006: 251, emphasis in original). It is achieved in part by the shift from government through explicit laws to discursive (self-)governance by multiple stakeholders through the operation of codes, norms, standards, guidelines and the like (Lunt and Livingstone 2007). The value of a 'talking shop', which some (non-binding) organizations – both international (e.g., Council of Europe) or multi-stakeholder (e.g., Internet Governance Forum) and with or without self-regulatory responsibilities – are sometimes denigrated for being, can be recognized better once it is understood that as governments step back from state control, the self-regulation that takes its place must be achieved through discursive means (rather than enforced

compliance). Consider the task of building a consensus if norms are to be voluntarily adhered to, as in the European Union's Guidance on Social Networking Sites; or the UK's Home Secretary's Task Force for Child Protection on the Internet;[15] or the Internet Watch Foundation's positive promotion of organizations that implement the Clean Feed blocking of illegal child sexual abuse images (IWF 2009).

One much-cited argument in favor of self-regulation is that industry can keep pace with technological developments more effectively than governments (which face a 'knowledge gap', as Schulz and Held (2006) put it, in the information sector, including regulator ignorance of the full array of entities to be regulated). The Chief Executive Officer (CEO) of the Family Online Safety Institute in the US observes that:

> 'as we catch up with and provide solutions to technologies and content that could prove harmful to kids, new devices, new strange meeting places spring up and thwart our earlier efforts' (Balkam 2008: 4).

One example of the need for constant updating of regulation, recently raised by the European non-governmental organization Alliance for Child Safety Online,[16] is how quickly the 2007 European Framework for Safer Mobile Use by Younger Teenagers and Children, albeit now implemented across 81 operators in 26 Member States (PricewaterhouseCoopers 2009), became outdated, failing to anticipate the risk of children being tracked using new generation location services (currently) outside the control of mobile operators (via Global Positioning System or GPS, wifi hotspots or Open Cell ID). Another is the continuing struggles between Facebook and its users over the appropriate management of privacy settings, illustrating the tension between making personal information public (to enable connections), as favored by Facebook and many of its adult users, and the contrary desire to keep personal information private (to enable intimacy), as favored by some adults, most parents and those concerned to protect children. Here it is generally deemed more effective for the industry and users to negotiate an appropriate balance rather than require regulators to intervene, though the digital literacy and social coordination skills required for this should not be underestimated.[17]

A second claim made by advocates of self-regulation is that the potential for multi-stakeholder self-determination and public participation are commensurately enhanced (although Schulz and Held (2006) argue the contrary). The discursive tone (if not necessarily the actual practice) of the emerging regulatory regime is illustrated by the United States' Department of Commerce in relation to the 'multi-stakeholder, private sector led, bottom-up policy development model' represented by ICANN.[18] As Künzler (2007: 354) observes, self-regulation works best if the following are in place:

> '(1) independence of self-regulation organizations from the regulated industry; (2) acceptance of self-regulation by the regulated companies and professionals; (3) sufficient funding and personnel resources; (4) clear definition of the procedures and goals of the self-regulation organisation and its transparency to the public'.

Regarding this last point, national and international organizations increasingly, it seems, conduct public consultations on their remit, codes and achievements, also facilitating public attitude research, stakeholder meetings and public events. Although

there are both principled and practical benefits to transparency and public deliberation, it is often observed that take-up from diverse and new voices can be disappointing, with a group of 'usual suspects' attending each event to express views that reflect and promote rather than revise their original position, and with few cases of change resulting from wider public participation. Doubts occur regarding the former points also, with the requirement for independence of the regulator from its sector seemingly elusive in the domain of children's online safety. This may be because the next two points (acceptance and funding) mitigate against such independence: an industry that provides the resources and the legitimacy for a regulator generally wishes to shape its work.

Take the case of the UK's Internet Watch Foundation, described as 'an independent, self-regulatory organisation' (IWF 2009a)[19] which provides a hotline and notice-and-take-down service for potentially illegal online content (generally, child sexual abuse images), part funded by the EC Safer Internet Programme and part of an international network of similar hotlines. Although the IWF is generally seen as a successful regulator, it is arguable that public legitimacy was not achieved, indeed was much contested internally and externally, until the Sexual Offences Act 2003 established a 'memorandum of understanding'[20] which officially recognized the organization's public policy goals (i.e., for child protection, thereby also precluding 'remit creep' into other kinds of speech, including that which is harmful but legal). Also important was the potential liability to prosecution of companies not operating the take-down service or, later, not centrally blocking sites listed by the IWF as potentially illegal.[21] In other words – an organization that proclaims itself self-regulatory nonetheless requires, in Held's (2007: 357) terms, 'a legal connection between the non-state regulatory system and the state regulation'; further, 'the state uses regulatory resources to influence the outcome of the regulatory process' – a case of co-regulation, in short.

Without a co-regulatory framework, it appears that not only legitimacy but also independent monitoring and compliance/enforcement are weakened in the move from government to governance. The industry's reluctance to subject itself to independent monitoring or evaluation of the effectiveness of its regulatory initiatives is a persistent feature of deliberation in this field. As Brown (in press) observes,

> 'while these [self-regulatory] schemes are more flexible and less burdensome than statutory regulation, they commonly lack the procedural fairness and protection for fundamental rights that are encouraged by independent judicial and parliamentary scrutiny'.

Nonetheless, the European Commission is undertaking some independent evaluation and monitoring – examples include the European mobile framework (PriceWaterhouseCoopers 2009) and the effectiveness of domestic filtering tools (DeLoitte and European Commission 2008). Monitoring the 2009 Safer Social Networking Principles for the EU (European Commission 2009a), to which most social networking services are signatories, proved more controversial – perhaps because many of the global players (e.g., Facebook, MySpace, Bebo, etc.) have their headquarters in the US. The UK Council for Child Internet Safety (UKCCIS) has found reaching agreement on the independent monitoring of codes of conduct or

guidance difficult, although its strategy statement of December 2009 does promise that:

> 'we will make sure that a review of how we are using each set of guidance is carried out periodically …reviews will be carried out by someone impartial with the right understanding and experience' (UKCCIS 2009: 11).

It adds that this is a matter of 'effective self-regulation', though it remains uncertain how effective such reviews will be. Thus, although the UK claims to lead in European and even wider international deliberations, having demonstrated the merits of multi-stakeholder cooperation to achieve self-regulation, there are signs that the European Commission and other international bodies may take the lead in pressuring national governments and indeed, major companies (Reid 2009).

Regulating Contact, Content and Conduct Risks Online

How, in practice, are online risks to children being regulated? Recalling EU Kids Online's threefold classification of online risks to children, as adopted by the UK's *Byron Review* ('Safer Children in a Digital World', commissioned by the Prime Minister; Byron 2008), it seems that contact risks, especially online grooming and paedophile activity, concern phenomena for which society has little or no tolerance and which are widely addressed by criminal law (Palmer and Stacey 2004; Quayle and Taylor 2005; Finkelhor 2008). Distributing photographs of child sexual abuse or grooming a child online in order to abuse him or her sexually is internationally regarded as unacceptable, though these are not illegal – and certainly not effectively prevented - everywhere. However, legislative solutions are generally sought only for high risk circumstances, for their effect is to constrain freedoms by making a wider set of actions illegal than would inevitably result in harm if permitted: for instance, children make many contacts online and only a few result in harmful encounters, albeit these may be disastrous for their victims.[22] Indeed, most online contacts afford positive experiences for children, valuable as part of their 'freedom of assembly'.

It is this, over and above the challenges of international law enforcement, which complicates the regulatory task of minimizing 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. Nor finally, are the available solutions unproblematic: is it best to scare parents into checking on their child's personal contacts, or to try to teach children complicated technical means of protecting their privacy, or to ensure the location of 'report abuse' buttons on every social networking and instant messaging service, or to require online providers to pre- or post-moderate all chat involving children, or… the list of possibilities could be continued, and few have yet been evaluated.

By contrast with contact risks, 'content is by far the most contentious area of media policy' (Freedman 2008: 122). Difficult questions of community standards and cultural values are vastly exacerbated in a transnational context (Millwood Hargrave, and Livingstone 2009; Preston 2009). Yet there is 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 (Waskul 2004).

Although traditionally tolerated in print or film, children's access to such content has traditionally been restricted, whether through regulatory or social means. 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 white lists, black lists, walled gardens, international content rating systems, more or less subtle filters applied at different points in the distribution chain or, last but not least, outright censorship, most initiatives have failed. An early failure was the attempt to establish a Dot Kids domain (under the US domain – .kids.us).[23] Although some countries' attempts to build children's walled gardens or portals have been more successful, especially among younger children (e.g., the German portal fragFinn connects to 4,000 sites and is widely used by children).

To be effective, such initiatives depend on considerable resources (to pre-moderate and update linked sites, and to mount public awareness campaigns so parents and children know of them). Resources are more readily forthcoming in large language communities and when provision is commercially rather than publicly funded, this tending to trade personal safety (from sexual or violent content) against children's freedom from commercial messages. Given ever-present resistance to censorship, content regulation is increasingly focused on the end user, notably through the provision of parental tools. Although, as Thierer (2009) observes, these depend both on effective design (neither over- nor under-blocking) and on 'good' parenting (i.e., assuming parents are not incompetent, overburdened, negligent nor ill-intentioned) (see also Oswell 2008). A particular and persistent problem is that of age verification: paraphrasing the widely cited *New Yorker* cartoon that nobody would know from your online activities if you were a dog, it is also the case that nobody knows if you are a child (notwithstanding various failed attempts, technical or regulatory, to enforce one to make such a distinction; Thierer 2009). Since children's preference is to spend time on generalist sites[24] where their presence is not generally detectable, their online experiences (including possible harm) are shaped by the commercial practices of major global players who are not easily subjected to the jurisdiction of individual nation-states.

'Sticks and stones may break your bones…'. Is it the case that, as the playground rhyme would have it, 'words can never hurt you'? As the risk agenda is broadened to encompass not only how adult society may harm children but also how children may attack each other (and, on occasion, victimize themselves), conduct risks raise exactly this question. For example, bullying has long been understood as including physical as well as verbal harassment among peers – what does this mean for cyberbullying? 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), 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 and Tippett 2006).

Cyberbullying is exacerbated by the ease of manipulating visual images, the extraordinary rapidity by which these may be spread, and the reach of such messages into the victim's private and supposedly safe places (his or her bedroom, on the phone, at home; boyd 2008). Add to this young people's reliance on the internet to

conduct their social relations, and the facility with which social networking sites bring together multiple forms of online communication, enabling all forms of contact from the most intimate to the widest of friendship circles, including hostile and abusive peer communication as part of the wider picture. In regulatory terms, conduct risks are the least amenable, for they occur peer-to-peer, not necessarily evident to observing (or supervising) adults. 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 (help-lines). In relation to conduct risks, the main effort is thus directed at making young people themselves, rather than industry, self-regulating, albeit with support from the state (and, acting on its behalf, schools).

Integrating Diverse Policy Initiatives

How might these currently piecemeal initiatives come together? And how might they tread the fraught path between the Scylla and Charybdis of top-down intervention by governments and laissez-faire reliance on the wisdom of users, the general public. One way is to conceive of improving safety less through the imposition of rules and regulations as by building safety considerations into the design and construction of the online environment (as already occurs in the offline environment, where this approach is established in engineering, urban planning, health and safety at work, and other domains). This seeks to anticipate the risks likely to be encountered (or even occasioned) by users and so incorporates risk and safety considerations into the design stages of innovation, planning and manufacture. Applied to the internet, what we might then call a policy of 'safety by design' recognizes that the public (including parents, children and those whose activities might harm children, intentionally or otherwise) is engaged with an environment that has been substantially planned for, designed, paid for and institutionally supported in particular ways, according to particular anticipated uses and in order to further particular interests (Mansell and Silverstone 1996). In other words, the online environment could have been and could yet be arranged otherwise, possibly reducing risk without disproportionate cost to the freedoms and opportunities of either children or adults.

In internet safety policy for children, this is to go beyond the widespread analogy of road safety (e.g., Criddle 2006; UKCCIS 2009), namely that just as society teaches children to cross roads safely it could teach them to use the internet safely. Rather, safety depends on a more fundamental interdependence of users and environments: children can only learn to cross roads designed with safety embedded into their physical design (traffic lights, width restrictions, road bumps, marked crossing points) and social rules (consider the public's familiarity with the rules of the road and society's enforcement of those rules). We do not teach children to cross a four lane highway or an unlit road at night or a road on which the cars have no vehicle testing, insurance or drink/drive laws. Thus, one must extend the road safety analogy to encompass that of town planning (Livingstone 2009). Only in the context of a planned environment, where children's playgrounds do not open onto major roads, sex shops are not sited next to schools, and commercial areas are regulated differently from residential ones, do we teach children how to treat strangers or travel where they need to go or with whom they can play freely. Interestingly, this balance of regulation and education is not generally resisted as a restriction on adult freedoms or as sacrificing the market to child protection – perhaps, because offline the planning system evolved

over generations, its principles and practices being gradually embedded in everyday 'common sense'.

Online, the regulatory regime is being developed much faster, permitting little time to attend to competing views, let practices settle down or wait for unintended consequences to unfold. Yet many of the regulatory practices referred to in this chapter are, as for town planning, attempts to manage conditions of accessibility – in this case, designing into websites and services enablers and constraints on what (or who) children (and others) can access and how. Examples, as noted throughout this chapter, include provision of filters, specification of child-friendly default settings, age verification systems, content rating and labelling, design standards, opt-in/opt-out points (e.g., for 'adult' content), and many more. Another aspect of the town planning analogy is important: when planning regulations are contested, there is recourse to an independent, transparent and public process of management and arbitration, including published codes of practice and a clear appeals process, whereby competing interests are fought out. Online, equivalent citizen protections are not yet widely in place. And even though large companies invest heavily in 'customer care' procedures, public accountability regarding their complaint handling, filtering decisions or moderation processes is rarely available to scrutiny. Sceptics will note further, that offline, planning processes are far from infallible – road accidents still happen, and crime, including crimes against children, are widespread. Nonetheless, such processes are vital to the infrastructure of society and, where lacking online, most countries hope or plan to introduce them.[25]

Conclusion

The internet promises wonderful opportunities for education, communication, participation and creativity. Yet the very same medium represents the means of bringing into the privacy of the home the very worst of society. This chapter has traced some of the debates, decisions and dilemmas encountered by diverse stakeholders across state, business and third sector as they acknowledge that children's experience of the internet and, therefore, for this reason (among others), the internet itself is being and must be regulated, in one way or another, albeit often with new problems arising just as old ones are resolved.[26] As we have seen, in these debates 'children' figure in several ways. Some arguments are traditional: throughout the history of media technologies, children's distinctive vulnerabilities and consequent need for protection against media harms have always been prominent, though the impulse to regulate has often mutated into efforts to educate (i.e., to promote media literacy; Drotner 1992). Some arguments are new: with the advent of interactive media, the user's agency is better recognized – though as a result, children's competence may be exaggerated (- 'digital natives', so called) or seen as dangerous (- 'hooligans' online as, supposedly, offline).[27] Some arguments are largely rhetorical: 'children' may be introduced into the public fray not so much to represent their interests as to provide a morally acceptable face for censorship (for restrictions on freedom of expression introduced to protect children may subsequently be used to restrict other forms of speech).

Although child protection is still sometimes framed as a limitation on adult rights to expression, legitimate or otherwise, it is a matter of children's rights, and when the rights of one segment of society conflict with the rights of another, some qualification

of absolute rights is the inevitable outcome. The policy dilemma then, concerns the appropriate balance among competing rights.

I have argued against any simple confrontation between adult freedoms and child protection, a confrontation in which children's rights – for both empowerment and protection – are unlikely to be supported. In refocusing instead on the more difficult balance between empowerment and protection in advancing children's interests specifically (though potentially wider public interests too), I have suggested that a more nuanced and proportionate approach to complex and competing rights and interests may emerge. Nonetheless, in certain regards it may be that conflicts between adult freedoms and child protection will remain, and in such cases it must be acknowledged there are as yet no ready answers.

As we also have seen, regulatory regimes are moving towards a 'softer', more indirect approach that disperses the role of the state by establishing more accountable national and transnational regulatory bodies, by engaging civil society in processes of governance and by encouraging in the 'responsible' or 'empowered' citizen the new task of personal risk assessment – 'the need to adopt a calculative prudent personal relation to fate now conceived in terms of calculable dangers and avertable risks' (Rose 1996: 58). But, countering enthusiasm for self-regulation, we have observed good reasons to support co-regulation even though, as Schulz and Held (2006: 63) caution, 'the effectiveness of the approach has to be examined in each case'. Nor is legislation always avoided: in the case of efforts to eradicate paid-for and peer-to-peer transactions in images of child sexual abuse, for instance, several countries have implemented specific legislation over and above the generic principle that, since those perpetrating crimes and those harmed by them live within national jurisdictions, 'what is illegal offline is illegal online' (Van Dijk 2006).[28] Each of these regulatory solutions has been much debated, for 'not only have media and culture industries become increasingly central in the economies of European countries, they have also become the terrain of contestation and consensus regarding self-governance and cultural identity' (Sarikakis 2007: 14).

In concluding this chapter, I must acknowledge the dangers of telling history from the midst of events, without the benefit of hindsight. Still, it is tempting to do so now that child online safety appears finally, though hardly centrally or uncontroversially, on the agenda of the Internet Governance Forum, the Organisation for Economic Co-operation and Development (OECD), the International Telecommunication Union, the European Commission and the Council of Europe, as well as many national governments around the world.[29] A recent survey of policies in place suggests considerable diversity in governance regimes worldwide, although more work is required to reach conclusions about whether regulation is effective in meeting public policy goals.[30] It seems, at least in developed countries, there may come a time when international models of regulation will influence, rather than merely recognize, coordinate and/or respond to, the regulatory regimes of individual nation-states. For researchers tracking children's experiences, both beneficial and harmful, for children's welfare and rights activists, and for parents and children themselves, these shifts pose new challenges regarding participation, transparency and accountability of the regulatory process as they - we - seek to understand the emerging mediated landscape and to identify the possible pressure points for change.

References

Alao, A. O., Soderberg, M., Pohl, E. L., and Alao, A. L. (2006) "Cybersuicide: Review of the role of the Internet on suicide", *Cyberpsychology & Behavior*, 9(4): 489-493.

All Party Parliamentary Communications Group (2009) *"Can we keep our hands off the net?" Report of an Inquiry by the All Party Parliamentary Communications Group*. London: apComms.

Balkam, S. (2008) *State of Online Safety Report*. Washington, DC: Family Online Safety Institute.

Barak, A. (2005) "Sexual harassment on the Internet", *Social Science Computer Review*, 23(1): 77-92.

Bauwens, J., Lobe, B., Segers, K., and Tsaliki, L. (2009) "A shared responsibility -- Similarities and differences in the factors that shape online risk assessment for children in Europe", *Journal of Children and Media*, 3(4): 316 - 330.

Beck, U. (1986/2005) *Risk Society: Towards a New Modernity*. London: Sage Publications.

Bennett, S., Maton, K., and Kervin, L. (2008) "The 'digital natives' debate: A critical review of the evidence", *British Journal of Educational Technology*, 39(5): 775-786.

Bohman, J. (1991) *New Philosophy of Social Science: Problems of Indeterminacy*. Cambridge: Polity Press.

boyd, d. (2008) "Why youth ♥ social network sites: The role of networked publics in teenage social life", in D. Buckingham (ed) *Youth, Identity, and Digital Media*. Cambridge: MIT Press, pp. 119–142.

Brown, I. (2008) "Internet filtering - be careful what you ask for", in S. Kirca and L. Hanson (eds) *Freedom and Prejudice: Approaches to Media and Culture*. Istanbul: Bahcesehir University Press, pp. 74-91.

Brown, I. (in press) "Internet self-regulation and fundamental rights", *Index on Censorship*.

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.

CEOP (2009) *Strategic Overview 2008-2009*. London: Child Exploitation and Online Protection Centre.

Christou, G., and Simpson, S. (2006) "The internet and public-private governance in the European Union", *Journal of Public Policy*, 26(1): 43-61.

Collier, A. (2009) "School cyberbully wins free-speech case", *NetFamilyNews.org*,, accessed 01/03/2010, http://www.netfamilynews.org/2009/12/school-cyberbully-wins-free-speech-case.html .

Collins, R., and Murroni, C. (1996) *New Media, New Policies: Media and Communications Strategies for the Future*. Cambridge: Polity Press.

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 .

Communications Consumer Panel (2009) *Response of the Communications Consumer Panel to the Government's consultation on legislation to tackle illegal peer-to-peer file-sharing*. London: Communications Consumer Panel, accessed

03/01/2010, http://www.communicationsconsumerpanel.org.uk/Response%20to%20online%20copyright%20infringement%20consultation.pdf .
ConnectSafely (2009) "Online safety 3.0: Empowering and protecting youth", *ConnectSafely.org*, accessed 01/01/2010, http://www.connectsafely.org/Commentaries-Staff/online-safety-30-empowering-and-protecting-youth.html .
Council of Europe (2007) *Building a Free and Safe Internet: Council of Europe Submission to the Internet Governance Forum, Rio de Janeiro, 12 to 15 November 2007*. Strasbourg: Council of Europe, accessed 03/01/2010, http://www.coe.int/t/dc/press/source/CoE%20submission%20to%20IGF_100807FINAL.doc .
Council of Europe (2009) "The promotion of Internet and online media services appropriate for minors", Parliamentary Assembly Council of Europe. Strasbourg: Council of Europe, accessed 03/01/2010, http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta09/EREC1882.htm .
Criddle, L. (2006) *Look Both Ways: Help Protect Your Family on the Internet*. Redmond: Microsoft Press.
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 .
Dahlgren, P., and Olsson, T. (2008) "Facilitating political participation: Young citizens, Internet and civic cultures", in K. Drotner and S. Livingstone (eds) *International Handbook of Children, Media and Culture*. London: Sage Publications, pp. 493-507.
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 .
Department for Culture, Media and Sport (2005) "Tessa Jowell keynote speech to the Creative Economy conference", London: Department for Culture, Media and Sport, assessed 01/01/2010, http://webarchive.nationalarchives.gov.uk/+/http://www.culture.gov.uk/global/press_notices/archive_2005/creative_economy_conference.htm .
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.
Drotner, K. (1992) "Modernity and media panics", in M. Skovmand and K. C. Schroeder (eds) *Media Cultures: Reappraising Transnational Media.* London: Routledge, pp. 42-62.
European Commission (2009) "Safer Internet Work Programme 2009", Brussels: Commission of the European Communities, accessed 03/01/2010, http://ec.europa.eu/information_society/activities/social_networking/eu_action

/selfreg/index_en.htm .
European Commission (2009a) "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 .
Federal Communications Commission (2008) "Children's educational television", Washington DC: FCC, accessed 01/01/2010, http://www.fcc.gov/cgb/consumerfacts/childtv.html .
Federal Communications Commission (2009) "Notice of inquiry in the matter of 'Empowering Parents and Protecting Children in an Evolving Media Landscape' ", Washington DC: FCC, accessed 10/12/2009, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-94A1.pdf .
Finkelhor, D. (2008) *Childhood Victimization: Violence, Crime, and Abuse in the Lives of Young People*. Oxford: Oxford University Press.
Frau-Meigs, D., and Torrent, J. (2009) "Media education policy: Towards a global rationale", in D. Frau-Meigs and J. Torrent (eds) *Mapping Media Education Policies in the World: Visions, Programmes and Challenges*. New York: The United Nations-Alliance of Civilizations & Grupo Comunicar, pp. 15-21, accessed 03/01/2010, http://portal.unesco.org/ci/en/ev.php-URL_ID=28540&URL_DO=DO_TOPIC&URL_SECTION=201.html .
Freedman, D. (2008) *The Politics of Media Policy*. Cambridge: Polity Press.
Govtrack.us (2008) "Broadband Data Improvement Act", accessed 01/01/2010, http://www.govtrack.us/congress/billtext.xpd?bill=s110-1492 .
Hamelink, C. J. (2008) "Children's communication rights: Beyond intentions", in K. Drotner and S. Livingstone (eds) *International Handbook of Children, Media and Culture*. London: Sage Publications, pp. 508-519.
Hasebrink, U., Livingstone, S., and 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/ .
Held, T. (2007). Co-regulation in European Union member states. *Communications*, 32, 415-422.
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 Crime Forum. (2000). *Chat Wise, Street Wise: Children and Internet Chat Services*. London: The Internet Crime Forum IRC sub-group.
Internet Governance Forum (nd) "Dynamic coalition on child online safety", *Internet Governance Forum*, accessed 01/01/2010, http://igf.wgig.org/cms/index.php/dynamic-coalitions/79-child-online-safety .
Internet Safety Technical Task Force (ISTTF) (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: Berkman Center for Internet and Society, Harvard University.

Ito, M., Horst, H., Bittanti, M., boyd, d., Herr-Stephenson, B., Lange, P. G., *et al*. (2008) *Living and Learning with New Media: Summary of Findings from the Digital Youth Project*. Chicago: The John D. and Catherine T. MacArthur Foundation.

IWF (2007) "Sex Offences Act 2003 memorandum of understanding", *Internet Watch Foundation*, Cambridge: IWF, accessed 01/01/2010, http://www.iwf.org.uk/police/page.22.213.htm .

IWF (2008) *2007 Annual and Charity Report*. Cambridge: Internet Watch Foundation.

IWF (2009) "IWF facilitation of the blocking initiative", *Internet Watch Foundation*, Cambridge: IWF, accessed 01/01/2010, http://www.iwf.org.uk/public/page.148.htm .

IWF (2009a) "IWF status", *Internet Watch Foundation*, Cambridge: IWF, accessed 01/01/2010, http://www.iwf.org.uk/public/page.103.549.htm .

Jessop, B. (2002) *The Future of the Capitalist State*. Cambridge: Polity Press.

Jowell, T. (2006) "Speech to the Oxford Media Convention", accessed 01/01/2010, http://www.ippr.org.uk/uploadedFiles/events/Tessa%20Jowell%20Speech.doc

Kotler, S. (2009) "Cyberbullying Bill could ensnare free speech rights", *Fox News*, New York: Fox News Network, LLC., accessed 01/01/2010, http://www.foxnews.com/politics/2009/05/14/cyberbullying-ensnare-free-speech-rights .

Künzler, M. (2007) "The state as a key success factor for self-regulation? Empirical evidence in brief", *Communications: The European Journal of Communication Research*, 32(3): 349-355.

Lenhart, A. (2009) *Teens and Sexting*. Washington, DC: Pew Internet & American Life Project.

Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York: Basic Books.

Livingstone, S. (2008) "Engaging with media – a matter of literacy?" *Communication, Culture and Critique*, 1(1): 51-62.

Livingstone, S. (2009) *Children and the Internet: Great Expectations, Challenging Realities*. Cambridge: Polity Press.

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

Livingstone, S., and 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/ .

Lobe, B., Livingstone, S., and Haddon, L. (2007) *Researching Children's Experiences Online across Countries: Issues and Problems in Methodology*, London: EC Safer Internet plus programme.

Lunt, P., and Livingstone, S. (2007) "Regulating markets in the interest of consumers? On the changing regime of governance in the financial service and communications sectors", in M. Bevir and F. Trentmann (eds) *Governance, Citizens, and Consumers: Agency and Resistance in Contemporary Politics.* Basingstoke: Palgrave Macmillan, pp. 139-161.

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

Mansell, R., and Silverstone, R., eds. (1996) *Communication by Design: The Politics of Information and Communication Technologies*. New York: Oxford University Press.

Millwood Hargrave, A., and Livingstone, S. (2009) *Harm and Offence in Media Content: A Review of the Empirical Literature* (Second edition). Bristol: Intellect Press.

Montgomery, K. C. (2007) *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet*. Cambridge: MIT Press.

Muir, D. (2005) *Violence Against Children in Cyberspace: A Contribution to the United Nations Study on Violence Against Children*. Bangkok: ECPAT International.

Murray, A. (2007) *The Regulation of Cyberspace: Control in the Online Environment*. Abingdon: Routedge-Cavendish.

National Campaign to Support Teen and Unplanned Pregnancy (2008) *Sex and Tech: Results from a Survey of Teens and Young Adults*. Washington, DC: National Campaign to Support Teen and Unplanned Pregnancy, accessed 03/01/2010, http://www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf .

NeuStar Inc. (2003) *Kids.us Content Policy: Guidelines and Restrictions*. Sterling: NeuStar Inc.

Nightingale, V., Dickenson, D., and Griff, C. (2000) *Children's Views about Media Harm*. Sydney: University of Western Sydney, Australian Broadcasting Authority.

O'Connell, R., and Bryce, J. (2006) *Young People, Well-Being and Risk On-Line*. Strasbourg: Media Division, Directorate General of Human Rights, Council of Europe.

Ofcom (2009) *UK Children's Media Literacy 2009 Annex: Top 50 Websites Visited by Children*. London: Ofcom, accessed 02/01/2010, http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/uk_childrens_ml/ .

Oswell, D. (2008) "Media and communications regulation and child protection: An overview of the field", in K. Drotner and S. Livingstone (eds) *International Handbook of Children, Media and Culture*. London: Sage Publications, pp. 475-492.

Palmer, T., and Stacey, L. (2004) *Just One Click: Sexual Abuse of Children and Young People Through the Internet and Mobile Telephone Technology*. Ilford: Barnardo's.

Pearson, G. (1983) *Hooligan: A History of Respectable Fears*. London: Macmillan.

Petley, J. (2009) "Web control", *Index on Censorship*, 38(1): 78-90.

Preston, C. B. (2009) "All knowledge is not equal: Facilitating children's access to knowledge by making the internet safer", *International Journal of Communications Law & Policy*, Winter(13): 115-132.

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 .

Quayle, E., and Taylor, M. (2005) *Viewing Child Pornography on the Internet: Understanding the Offence, Managing the Offender, Helping the Victims*. Lyme Regis: Russell House.

Raboy, M., and Shtern, J. (2010) "Mediated speech and communication rights: Situating cyber-bullying within the emerging global Internet governance regime", in S. Shariff and A. Churchill (eds) *Truths and Myths of Cyber-bullying: International Perspectives on Stakeholder Responsibility and Children's Safety*. New York: Peter Lang, pp.193-226.

Reding, V. (2009) *How Can We Empower Youngsters to Stay Safe Online? Innovative Solutions in Europe*. Stockholm: World Childhood Foundation Seminar, accessed 02/01/2010, http://ec.europa.eu/commission_barroso/reding/docs/speeches/2009/stockholm-170909.pdf .

Reid, A. S. (2009) "Online protection of the child within Europe", *International Review of Law, Computers & Technology*, 23(3): 217 - 230.

Rose, N. (1996). "Governing 'advanced' liberal democracies", in A. Barry, T. Osborne and N. Rose (Eds.), *Foucault and Political Reason: Liberalism, Neo-Liberalism and Rationalities of Government* (pp. 37-64). London: UCL Press.

Sarikakis, K., ed. (2007) *Media and Cultural Policy in the European Union*. Amsterdam: Rodopi.

Schulz, W., and 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*. Göteborg: Nordicom, pp. 49-65.

Scott, C. (2001) *Analysing Regulatory Space: Fragmented Resources and Institutional Design*. London: Sweet & Maxwell.

Shariff, S. and Churchill, A., eds. (2010) *Truths and Myths of Cyber-bullying: International Perspectives on Stakeholder Responsibility and Children's Safety*. New York: Peter Lang.

Smith, P., Mahdavi, J., Carvalho, M., and Tippett, N. (2006) *An Investigation Into Cyberbullying, Its Forms, Awareness and Impact, and the Relationship Between Age and Gender in Cyberbullying*. London: The Anti-Bullying Alliance.

Staksrud, E. (2009) "Problematic conduct: Juvenile delinquency on the Internet", in S. Livingstone and L. Haddon (eds) *Kids Online: Opportunities and Risks for Children*. London: Policy Press, pp. 147-158.

Szoka, B., and 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., and 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 .

UKCCIS (2009) *Click Clever Click Safe. The First UK Child Internet Safety Strategy*. London: UK Council for Child Internet Safety, accessed 03/01/2010, http://www.dcsf.gov.uk/ukccis/download.cfm?catstr=research&downloadurl=UKCCIS%20Strategy%20Report-WEB1.pdf .

UNICEF (1999) "The Oslo challenge", New York: UNICEF, accessed 28/3/07, http://www.unicef.org/magic/briefing/oslo.html .

United States Federal Trade Commission (1998) *Children's Online Privacy Protection Act 1998*,15 U.S.C. § 6501–6506, Public Law 105-277, 112 Stat. 2581-728, enacted October 21, http://www.ftc.gov/ogc/coppa1.htm accessed 12 Feb 2010.

Van Dijk, J. A. G. M. (2006) “Law”, in J. A. G. M. Van Dijk (ed) *The Network Society: Social Aspects of New Media*. London: Sage Publications, pp. 127-155.

Vygotsky (1934/1986) *Thought and Language*. Cambridge: MIT Press.

Waskul, D. D. (2004) *Net.seXXX: Readings on Sex, Pornography, and the Internet*. New York: Peter Lang.

White House Office of the Press Secretary (2002) “President Bush signs child Internet safety legislation”, accessed 11/1/10, http://www.cms.kids.us/press/dotkids_news_12.04.02.pdf .

Willard, N. (2009) *There is No Constitutional Right to be a Cyberbully: Analysis of J.C. v Beverly Hills Unified School District*. Eugene: Center for Safe and Responsible Internet Use, accessed 03/01/2010, http://webhost.bridgew.edu/marc/JCcyberbullyingcase.pdf .

Willett, R. (2008) “Consumer citizens online: Structure, agency, and gender in online participation”, in D. Buckingham (ed) *Youth, Identity, and Digital Media*. Cambridge: MIT Press, pp. 49–69.

Wolak, J., Finkelhor, D., Mitchell, K. J., and Ybarra, M. L. (2008) “Online "predators" and their victims”, *American Psychologist*, 63(2): 111-128.

Wyatt, D. (2009) “Digital rights for children and the 20th Anniversary of the UN Convention on the Rights of the Child”, accessed 03/01/2010, http://www.derekwyatt.co.uk/news_item.aspx?i_PageID=117916 .

Zürn, M., and Koernig-Archibugi, M. (2006) “Conclusion II: The modes and dynamics of global governance”, in M. Koernig-Archibugi and M. Zürn (eds) *New Modes of Governance in the Global System: Exploring Publicness, Delegation and Inclusiveness.* Basingstoke: Palgrave Macmillan, pp.236-255.

Endnotes

[1] Parts of this chapter are adapted from material published in *Children and the Internet* (Livingstone 2009); other parts draw on conclusions from the EU Kids Online project (see www.eukidsonline.net). In writing this chapter, I was stimulated by a seminar held at the Oxford Internet Institute on *Child Protection, Free Speech and the Internet: Mapping the Territory and Limitations of Common Ground* (October 2010). I also draw on my experience in directing the pan-European research network, EU Kids Online, funded by the EC (DG Information Society) Safer Internet Programme, and advising Ofcom (the Office of Communications) during the UK Prime Minister's *Byron Review for Safer Children in a Digital World*, as well as my roles on the Ministerial Home Access Initiative, the Board of the Internet Watch Foundation and as chair of the Expert Research Panel of the newly formed UK Council for Child Internet Safety. By reflecting on insights derived from the academy, from advising government, and from working with a self-regulatory body, I hope to combine contextualised interpretation (in which the researcher draws on insider knowledge) and rational interpretation (in which the researcher draws on outsider knowledge), as advocated by Bohman (1991). I warmly thank those associated with the above organizations who have, in recent years, discussed with me the ideas expressed within this chapter and even checked some of the claims I make here – especially Stephen Balkam, John Carr, Anne Collier, Richard Collins, Jason De Bono, Leslie Haddon, Zoe Hilton, Peter Robbins, Elisabeth Staksrud and Damian Tambini; I also thank the editors of this volume for their comments on an earlier version.

[2] Consider analogous policies in the realm of mass media. These include the US's Children's Television Act 1990, which mandated three hours of educational television broadcasting for children per week on each channel; see also Federal Communications Commission (2008). In the UK, the considerable investment of the British Broadcasting Corporation (BBC) in children's resources online (http://www.bbc.co.uk/cbbc/) is widely envied in Europe and elsewhere although cross-media ownership rules to prevent so-called market distortion limit what public service broadcasters may provide for children online.

[3] For information about the Internet Governance Forum, see http://www.intgovforum.org/cms/.

[4] Specifically, the report called for a Privacy Bill, measures to address illegal file sharing, a call for opt-in (rather than opt-out) procedures for behavioral advertizing especially for children, for e-safety teaching in the core school curriculum, for point-of-sale e-safety messages for mobile phones, for child protection filters to be 'on' by default on new mobile handsets, for the Internet Watch Foundation's 'notice and take-down' mechanisms for illegal child sexual abuse images to be extended worldwide, for legislation to ensure all UK Internet service providers operate service-level blocking of such illegal images, for continued support for network neutrality, for a minimum guaranteed speed for domestic broadband connections, for a voluntary code for internet service providers to detect and deal with malware - to be followed by an imposed code if the voluntary system fails, and for a new law to encourage internet service providers to detect and remove inappropriate content without losing their 'mere conduit' legal immunity (see All Party Parliamentary Communications Group 2009). Similar calls come from the Communications Consumer Panel, affiliated to Ofcom – see, for example, its recent recommendation that legislation should require Ofcom to facilitate or, failing voluntary compliance, impose a Code of Conduct to protect consumer rights against stringent penalties (such as broadband disconnection) against illegal downloading; see Communications Consumer Panel (2009).

[5] This is currently being debated in the US House of Representatives (Kotler 2009). See Willard's (2009) analysis of the recent *J.C. v. Beverly Hills Unified School District* case. For a recent case to the contrary, see Collier (2009) and for a wider discussion, see Raboy and Shtern (2010).

[6] According to the EU E-Commerce Regulations 2002, a network operator is not legally liable for the consequences of traffic delivered via its networks.

[7] See also the Pew Internet & American Life Project survey (Lenhart 2009) finding that only four percent of 12-to-17-year-olds in the US had sent a sexually suggestive nude or semi-nude photo or video of themselves via cellphone; 15 percent had received one on their mobile from someone they know personally.

[8] The term online 'grooming' refers to the practice of befriending a child online with the intention of sexually abusing them. In 2008-9, the UK's Child Exploitation and Online Protection Centre (CEOP 2009: 38) which addresses the relation between online activities and child victims, reported that it had rescued 139 children from sexual abuse, produced intelligence reports which led to 334 arrests, and disrupted or dismantled 82 high risk sex offender networks. It also reported receiving 50-100 youth reports/month, most of them relating to sexual abuse/harassment (CEOP 2009: 18).

[9] See Title 2, Sect. 214 of the Broadband Data Improvement Act 2008 (Govtrack.us 2008).

[10] As asserted, ten years on again, by British MP Derek Wyatt, co-chair of the All Party Communications Group, in calling on the UN 'to work in cooperation with legislators and civil society to examine and assess whether the Convention on the Rights of the Child fully addresses the needs of children around the world in this digital age' (Wyatt 2009: nd).

[11] See Council of Europe (2007; 2009).

[12] See also Viviene Reding's claim that 'we need to stimulate the production, visibility and take-up of positive content online' (Reding 2009: nd).

[13] To those from the US, the UK, Germany or other wealthy countries with large language communities, this may seem unnecessary. But to children who speak Czech or Greek or Macedonian, very little indeed is available for them on the Internet (Livingstone 2009a). Again, political-economic arguments about public service broadcasting, distorting the market if extended online, have been prioritized over meeting children's right to engage with material in their own language, without advertizing or undue persuasion, and using the medium of their choice, as stated in the UN Convention on the Rights of the Child.

[14] In this regard, internet regulation contrasts with longer communication policy struggles. The public service broadcasting provision for example, or the universal service obligation - where a relatively coherent policy domain has traditionally been shaped by overarching (though still contested) principles (public value, universal service and universal access, the regulation of harmful and offensive content, restrictions on commercial messaging) - was managed, at least in the UK, by a broadly-trusted regulatory body. In the UK, this has generally been the BBC, Ofcom, and before that Oftel and the Independent Television Commission), all overseen by a distinct government ministry (again in the UK, Department of Media, Culture and Sport, although with substantial input from the Department for Trade and Industry, renamed Department for Business and Regulatory Reform, and now Department for Business, Innovation and Skills) (Collins and Murroni 1996; Freedman 2008).

[15] In the UK, the Home Secretary's Task Force for Child Protection on the Internet was set up in March 2001 following a report by the Internet Crime Forum (2000). It has produced widely implemented guidance – both in the UK and emulated elsewhere - regarding safety messages, searching, moderation of chat rooms and instant messaging, reporting of abuse and social networking services. This successfully sustained a multi-stakeholder dialogue sufficient to produce industry-accepted guidance on moderating interactive services, on the provision of chat, instant messaging and other web-based services used by children, and on safe search procedures and parental tools, much of it later implemented on a European and international level (e.g., Safer Social Networking Principles for the EU, European Commission 2009a). These and diverse other initiatives (e.g., a Kitemark for end user filtering software, guidance for social networking sites, internet safety materials for teachers and public awareness raising campaigns for parents) are now being coordinated by the UK Council for Child Internet

Safety, established by Prime Minister Gordon Brown in 2008 to implement the recommendations of *The Byron Review* (Byron 2008).

[16] See http://www.chis.org.uk/uploads/01.pdf .

[17] This is not to say existing legislation does not apply here - the US's Children's Online Privacy Protection Act 1998 (United States Federal Trade Commission (1998), which precludes the collection of personal information from children younger than 13 years of age without parental permission, has resulted in Facebook setting 13 as the lower age limit for registration.

[18] A 2009 statement saw ICANN commit 'to maintain and improve robust mechanisms for public input, accountability, and transparency so as to ensure that the outcomes of its decision-making will reflect the public interest and be accountable to all stakeholders' (ICANN 2009: nd).

[19] Lest one doubt the severity of this material, the organization (IWF 2008) reports that some 80 percent of internet sites hosting child sexual abuse images are commercial operations, and that 10 percent of the child victims being sexually abused – this including scenes of rape, in photographs or videos on these sites – appear to be under two years old; 33 percent appear between three and six years of age; and 80 percent appear to be under the age of ten (IWF 2008). IWF data show a trend towards increasing severity of the abuse portrayed, supporting the IWF's claim that 'behind every statistic is a child who has been sexually abused and exploited and, whilst images of the abuse are in circulation on the internet, that abuse is perpetuated' (IWF 2008: 8).

[20] See Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003 (IWF 2007).

[21] Indeed, there were suggestions in some quarters that failure to utilize the IWF list could potentially render a non-compliant ISP liable for hosting illegal content or even precipitate legislation to make such blocking compulsory (Brown in press).

[22] One challenging consequence of widespread Internet use is the extent to which youthful activities may be newly rendered illegal – from downloading music from peer-to-peer networks to circulating hate messages or producing indecent images of one's boy/girlfriend on a mobile phone.

[23] In 2002, this children's 'walled garden' appeared successful. When President Bush signed the Dot-Kids Implementation and Efficiency Act in the USA, he said: 'This bill is a wise and necessary step to safeguard our children while they use computers and discover the great possibilities of the Internet. Every site designated .kids will be a safe zone for children' (White House Office of the Press Secretary 2002: np). However, since dot.kids sites could not connect to any sites outside the domain (NeuStar Inc. 2003), few organizations invested in populating the domain and it is effectively inactive.

[24] For example, in the UK, the top ten sites visited by 6-11 year olds include Google, eBay, MSN, YouTube and Facebook (Ofcom 2009).

[25] As revealed by a survey conducted by the ITU's Child Online Protection initiative of the 191 Member States of the ITU in late 2009 (ITU 2009).

[26] For a balanced overview, see 'Online Safety 3.0: Empowering & Protecting Youth' (ConnectSafely 2009).

[27] Pearson (1983) develops a critique of the moral panic thesis in relation to the sociological emergence of hooligans, while Staksrud (2009) identifies the evidence that children and young people act as hooligans online – charting their activities in relation to cyberbullying, hacking, illegal downloading, plagiarism and so forth.

[28] Norway's laws, as well as that of the UK, against online grooming are examples of this: in the UK, this is Section 46 of the Sexual Offences Act 2003; in Norway, it is Norwegian Criminal Code § 201. Other examples include the Australian Cyber Stalking Law (1999) and the US's Children's Online Privacy Protection Act (1998); see also Montgomery (2007).

[29] See for example, the Internet Governance Forum's Dynamic Coalition on Child Online Safety, which aims '[t]o create a permanent, open platform for discussion on fundamental and practical issues related to child online safety within the agenda of the Internet Governance Forum, ensuring dialogue among representatives from children's organizations, government, industry, academia and other civil society groups' (IGF nd: np). See also the ITU's Child Online Protection initiative (ITU 2009), the Council of Europe's Recommendation 1882 (Council of Europe 2009), and also the current work of the OECD 'Working Party on Information Security and Privacy' on the protection of children online.

[30] See 'Answers to APEC Children Protection Project Questionnaire', APEC-OECD Joint Symposium on Initiatives Among Member Economies Promoting Safer

Internet Environment for Children, Singapore 15 April 2009, accessed 11/1/10, http://aimp.apec.org/Documents/2009/TEL/TEL39-SPSG-SYM/09_tel39_spsg_sym_018.pdf.