48

INTERNET POLICIES

Online child protection and empowerment in a global context

Brian O'Neill

Introduction

Children's use of the internet has in the first decade of the twenty-first century become a matter of major policy concern. With increasing numbers of young people going online at ever-younger ages and through diverse platforms, governments, NGOs and industry stakeholders have demonstrably increased the attention given to matters of safety and child protection online whilst grappling with rapidly changing trends and technological developments. Policy in this area is most often framed in terms of the need to balance the hugely important opportunities the internet offers children whilst recognising that as minors they require protection. In addition, internet policy for children cannot be separated from international debates on the regulation of the internet, internet freedom and growing trends towards censorship and control of information.

This chapter briefly reviews the principal contours of internet policy for children, charting the growing international consensus on the need to balance digital opportunities for young people with the attendant risks they inevitably encounter. Internet use here refers to all online activities undertaken by children and all the connected devices employed for going online.

Early approaches to online child protection

In what may be called the first phase of internet policy and regulation during the decade of the 1990s, the principal trend pursued was in fact that the internet should not be regulated at all and that, as a nascent medium, technological innovation would be best served by as little interference as possible. In contrast to a medium such as television where its impact on children was always a matter of public concern (Gunter and McAleer, 1997), the main policy priority in the early years of the internet was to promote greater access, harnessing educational opportunities and competitive economic advantage. However, as Lawrence Lessig notes, it did not take long for policymakers to become concerned about the rapid proliferation of pornography and other kinds of unsuitable content universally regarded as harmful for children (Lessig, 2006).

Efforts to introduce internet-specific legislation included the ill-fated Communications Decency Act of 1996 (CDA) in the United States, intended to restrict access by minors to online pornography or other explicit content and to regulate indecency and obscenity on the

internet according to 'community standards'. As initially passed by the US Congress in 1996, the CDA imposed criminal sanctions on anyone who:

> knowingly (A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or (B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs.
>
> *(Telecommunications Act of 1996, Pub. L. No. 104–104, tit. 5, 110 Stat. 56, 133–43, Sec. 502)*

Subsequently, its provisions against indecency were successfully challenged in the US Supreme Court (Reno v. ACLU), and an amended CDA without indecency provisions passed into US law. A further effort to restrict access by minors to pornography or any material that might be harmful to them was proposed in 1998 with the Child Online Protection Act (COPA) though it also was the subject of an injunction and never took effect. The final and ultimately successful measure, the Children's Internet Protection Act (CIPA), was signed into law in 2000 and required US schools and libraries as a condition of federal funding to use internet filters to restrict access by children to harmful online content.

A somewhat different approach emerged in Europe. The *Green Paper On The Protection Of Minors And Human Dignity In Audio-visual And Information Services* (European Commission, 1996a), for instance, was an early attempt to address child protection in the context of a converged media environment. At the same time, the communication on illegal and harmful content on the internet (European Commission, 1996b) laid the ground for a multi-stakeholder approach in tackling the problem of how to regulate content, observing that without effective controls, trust and confidence in the new communications environment would be damaged, constraining the potential benefits of the information society. The introduction of a multiannual Safer Internet Action Plan (European Commission, 1999, 2004) provided a further platform for the development of child protection policies, preferring where possible collaborative arrangements between stakeholders rather than direct legislative intervention. Accordingly, in parallel with the rapid expansion of the internet in the years following 2000, an ambitious series of measures to protect minors evolved through industry self- and co-regulation, filtering and content classification, networks of hotlines and helplines, as well as awareness-raising strategies and education about internet safety. Thus, it was recognised that there was no single solution to the challenges raised by mass use of the internet as well as the fact that, more and more, children and their families would be required to assume greater levels of responsibility for their own safety.

An emerging consensus on matters that affect children may be observed in the first 15 years or so of internet policy and regulation. There is, for instance, a common identification by governments and regulators around the world that children require protection from content that may be harmful to their development and this is the area that has attracted the most attention. In addition, online communication and participation in services originally designed for adults are also agreed to be risky. Similarly, children's own actions where young people themselves may be perpetrators of harmful behaviour are another area of risk. In response, a variety of strategies has emerged to regulate content and behaviour, whilst recognising that multiple actors share the responsibility for providing appropriate protective measures.

Regulating content

Protecting children from unsuitable content that may be harmful for their development is a cornerstone of internet policy for children. Determining which content is unsuitable for children and for which age groups, however, is contested. Illegal content, such as extreme xenophobic material and child sexual abuse imagery, falls into the category of illegal content in almost all jurisdictions. In such instances, what is deemed illegal in the offline world is illegal in the online world also and the only issue is one of ensuring effective compliance and the operation of applicable laws. For other content that may be deemed potentially harmful, but not illegal, provisions for protection vary considerably. Such content risks may include violent or gory online content as well in video games, 'adult' and other pornographic content, racist content or forms of hate speech, and forms of commercial content that may target children in ways for which they are not prepared (Livingstone and Haddon, 2009).

Regulation of content features prominently in the national audio-visual policy schemes of most countries and to some extent in online policy frameworks (OECD, 2011). A general ban on illegal content, offline and online, for instance, is provided for on a near-universal basis. In the United States and Canada, there is a tendency not to have internet-specific legislation governing content while others including Japan, Turkey and Korea have passed dedicated laws governing online content. Between these extremes, most European countries, and Australia and New Zealand, rely to a large extent on the application of existing laws augmented by 'soft' legislation in the form of self- and co-regulatory schemes to enforce age restrictions on content.

Content regulation regimes typically rely on forms of international cooperation between law enforcement, industry and other public–private partnerships in monitoring and suppressing, where applicable, illegal and criminal online content. Mandatory filtering at a national level is applied in only a limited number of countries (Turkey, and proposed in Australia). More frequently, it is applied on a voluntary basis, for instance, as recommended for countries within the European Union under the 2011 Directive on combating the sexual exploitation of children and child pornography (European Union, 2011). Filtering at the level of the internet service provider for content that is not illegal but is recognised as unsuitable for children is always voluntary, even in a country such as Turkey where overall strict censorship applies (OSCE, 2010).

Labelling and classification

An area of specific policy attention since the late 1990s has been the attempt to develop appropriate classification schemes for labelling online content in a way that will better enable parents to make judgements on the suitability of content and to make filtering systems more effective. In the European Union, developing effective and transparent labelling systems has been a feature of safer internet policy since the development of the first Safer Internet Action Plan. Concerns about the effects of violent video game content led to the first voluntary rating system for console games developed by the UK-based Entertainment Leisure Software Publishers Association (ELSPA) in 1994. However with the proliferation of nationally-based classification systems and consequent consumer confusion, the so-called Pan European Game Information system (PEGI) was introduced in 2003. The development of PEGI marks a shift from a legislatively-based classification system based on age-ratings, familiar to the traditional media environment, to one based on labelling, content descriptions and indications of age appropriateness (McLaughlin, 2007). The system is a voluntary one operated by manufacturers and game developers and includes age rating symbols (3+, 7+, 12+, 16+ and 18+) and content descriptors (bad language, discrimination, drugs, fear, gambling, sex and violence). Often seen as a success story for the approach of co-regulation, it has been adopted by most countries in Europe, with strong support from the European

Commission, and reinforces the legislative basis of games classification in countries such as Ireland and the UK.

Less successful have been attempts to extend content classification and labelling systems to the online sphere. PEGI Online, an addition to the PEGI system, was designed specifically for online gaming content using a similar labelling system and supported by an industry code of practice. The system has limited participation however. Other efforts to promote ratings systems for online content have included the Internet Content Rating Association (ICRA), the internationally structured self-regulation initiative (Machill et al., 2002). This content description system was intended to allow web developers to self-label content using categories such as:

- The presence or absence of nudity
- The presence or absence of sexual content
- The depiction of violence
- The language used
- The presence or absence of user-generated content and whether this is moderated
- The depiction of other potentially harmful content such as gambling, drugs and alcohol.

This descriptive classification scheme is operated by the self-completion of a questionnaire (the ICRA Questionnaire) and is intended for use with filtering systems to facilitate and support parental guidance in relation to young people's access to online content. First established in 1994, the system has gained limited industry support and as of 2010 has been absorbed within the Family Online Safety Institute (FOSI) organisation.

Contact risks

Contact risks in which children may be harmed by coming into contact with others via the internet is another area with which internet policy has been particularly concerned. In the main, the contact risks addressed by policymakers have been those in which children have been participants in adult-initiated activity, as an extension of those risks to children from exposure to content that is not age appropriate. 'Stranger-danger' and the risk of abuse of children by adults they may encounter online, while extremely rare, have created significant public anxiety and have subsequently featured in policy debates concerning the protection of children online. Legislative responses have focused on the most extreme forms of risk such as grooming and child sexual abuse facilitated via internet communication. In many countries, new legislative provisions outlawing cybergrooming as a new type of criminal offence have been developed (OECD, 2011, p. 33). The risks of mobile internet use and social networking have also received attention in developing countries where computer and broadband internet use is low but access to mobile phones is high (Beger et al., 2011).

Another dimension of contact risk that has received less attention is that of children's exposure to commercial communication (DCFS/DCMS, 2009). Where in traditional media, restrictions on advertising to children are well established, this is an aspect of the online world that is much less developed. Online gambling, however, in most countries cannot be offered to children. More generally, commercial communication is the subject of self-regulation and only in the Scandinavian countries is advertising to children banned.

Children as actors and perpetrators

The internet is also an interactive environment, especially so for children who are often enthusiastic participants in social media platforms, and the originators of content across the myriad

of web 2.0 services available to them. As such, internet policy has had to address questions of conduct initiated by children themselves where youth behaviour has led to new areas of risk and potential harm. Cyber harassment and cyberbullying, arising, more often than not, out of contact between peers, has attracted substantial attention as a persistent and at times intractable aspect of young people's online behaviour (Erdur-Baker, 2010). Cyberbullying – where it does not fall into the category of criminal harassment to which existing laws apply – is primarily addressed through awareness-raising strategies, focusing in particular on the offending and hurtful behaviour of perpetrators, coping strategies for victims and educational policies for target populations (Hinduja and Patchin, 2009; Shariff and Churchill, 2010). Relatedly, the phenomenon of 'sexting' or sending/receiving sexual messages via electronic communication, whether wanted or unwanted, is another area of contact risk that has received research and policy attention (Lenhart, 2009; Ringrose et al., 2012). It has received a more varied response, ranging from criminal prosecutions based on laws pertaining to possession of child pornography (Sacco, 2010) to a policy of 'turning a blind eye' to risky youthful practices.

Potentially harmful user-generated content is a relatively new area of risk where children and young people access or even originate content that includes racist or hate speech, drug-taking and the promotion of anorexia/bulimia, or talk about ways to commit suicide. While such content is subject to the terms of use adopted by the service providers concerned, calls for greater vigilance by hosting companies alongside increasing pressures towards content censorship are evident (Deibert, 2008).

Of course, the one area in which youth conduct has been the subject of most sustained policy action has been in relation to copyright infringement and illegal downloading of copyright content. US Federal Law in the form of the Digital Millennium Copyright Act (1998) exempts internet intermediaries from liability for content carried on their networks. However, increasing pressure from the music industry to tackle apparently widespread copyright infringement through peer-to-peer file sharing has focused efforts on requiring internet service providers (ISPs) to block access to sites facilitating illegal downloading and to cut off access to offending downloaders. This has been fiercely resisted by civil liberties groups opposed to any form of intermediary blocking and efforts to implement the so-called graduated response or 'three strikes policy' in different national jurisdictions, such as France and the United Kingdom, continue to be deeply contested (Ryan, 2010).

Alternative regulatory policy approaches

Legislation-based policy approaches to child protection online provide just one dimension of what is recognised as a complex set of public policy challenges. As such, a host of alternative regulatory instruments and strategies has been developed to address concerns for children's safety (Lievens, 2010). Given the open and dynamic nature of the internet, and the wide cultural variation in moral standards relating to children's exposure to online content, much policy emphasis has been placed on the importance of parents deciding what is best for their children. An early initiative in this regard was the promotion of technical solutions or software-based parental controls to restrict children's surfing. Despite concerns over their effectiveness as well as their suitability for older children and teenagers, parental controls have been a core feature of internet policy in many countries since the late 1990s and continue to be recommended as an important ingredient in the overall mix of digital safety (Deloitte and European Commission, 2008; Thierer, 2009).

Industry supported self-regulatory agreements have undoubtedly been amongst the most important non-legislative initiatives designed to promote safer internet practice. In the European

context, safer use of mobile communications as well as safer social networking have been the two key sectors in which industry providers have, with Commission support, developed a code of practice regarding child safety (European Commission, 2009; GSMA, 2007). Deemed to be the best equipped to respond to rapid changes in technology and the marketplace, industry operators outline their public commitments towards implementation of the agreed code or set of principles, which is then independently evaluated (see Donoso, 2011). Self-regulation, for long a foundation of new media policy, is however coming under increasing scrutiny due to perceived shortcomings in meeting public interest needs as well as difficulties associated with monitoring effectiveness and implementation (Bonnici and De Vey Mestdagh, 2005; Phillips, 2011).

Of most significance in the non-regulatory approach to internet safety has been the emphasis on awareness-raising and education. The education of young internet users is recognised as essential to empowering users and encouraging safer, more responsible online behaviour. Awareness-raising campaigns, with both public and private sector input, have been widely used to draw attention to issues of security and safety, while promoting specific safety messages regarding online use. Educational reinforcement in partnership with national education systems is seen as vital to improving levels of digital literacy and encouraging self-governing behaviour on the part of children and young people (Eurydice, 2009; Safer Internet Programme, 2009). Concepts such as digital citizenship are intended to reflect the importance of the rights and responsibilities of children as social actors in the online world (Mossberger et al., 2008; Passey, 2011) as well recognising that the best form of protection for young people is self-empowerment (O'Neill and Hagen, 2009).

Conclusion

Despite the evident importance now attached to the agenda of digital safety, and the strong consensus among international agencies both in combating abuses and in promoting online safety (ITU, 2009; UNICEF, 2011), unevenness remains a characteristic of the internet policy landscape with substantial differences at a geo-political level between proponents of an open internet, free of restrictions, whether for neo-liberal economic reasons or based on libertarian principles of free expression, and a more regulated and, in some cases, overtly controlled network. This occurs at a time of rapid internet expansion across the globe and the demonstrable proliferation of new, more accessible means of going online. Children's interests are often located somewhere in the middle of such developments, both as the early adopters and digital explorers of new technologies, and also as the subjects of intense debate on the need for protection, or even as justification for extreme forms of restriction. It is all the more important from a policy perspective, therefore, that children's welfare in the online world be incorporated as part of a wider policy in a converged media environment. This implies ~~therefore~~ that promoting equality of access and participation duly takes into account appropriate levels of protection afforded to all citizens, as well as those representing the best interests of the child, and that standards applying in the media environment as a whole are the outcome of a critical and reflective debate on the values of a responsible and ethical (digital) citizenship.

References

(no colon)

Beger, G., Hoveyda, P. K. and Sinha, A. (2011). From ~~:~~"What's your ASLR" to "Do you wanna go private?" New York: UNICEF.

Bonnici, J. P. M. and De Vey Mestdagh, C. N. J. (2005). Right vision, wrong expectations: The European Union and self-regulation of harmful internet content. *Information & Communications Technology Law*, *14*(2), 133–49.

DCFS/DCMS (2009). *The Impact of the Commercial World on Children's Wellbeing Report of an Independent Assessment*. London: DCFS/DCMS.

Deibert, R. (2008). *Access denied: the practice and policy of global Internet filtering*. Cambridge, MA: MIT.

Deloitte and European Commission (2008). Safer internet: Protecting our children on the net using content filtering and parental control techniques. Luxembourg: European Commission Safer Internet Programme.

Donoso, V. (2011). Assessment of the implementation of the safer social networking principles for the EU on 14 websites: Summary report. Luxembourg: European Commission, Safer Internet Programme.

Erdur-Baker, Ö. (2010). Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools. *New Media & Society*, *12*(1), 109–25.

European Commission (1996a). Green paper on the protection of minors and human dignity in audiovisual and information services. Brussels: European Commission.

——(1996b). Illegal and harmful content on the internet COM(96)487. Brussels-Luxembourg: European Commission.

——(1999). A multiannual community action plan on promoting safer use of the internet by combatting illegal and harmful content on global networks. 4-year work programme 1999–2002. Luxembourg: European Commission Safer Internet Programme.

——(2004). Safer internet action plan. Update of the work programme 2003–4 for the year 2004. Luxembourg: European Commission Safer Internet Programme.

——(2009). Safer social networking principles for the EU. Luxembourg: European Commission Safer Internet Programme.

European Union (2011). Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:026:0001:0021:EN:PDF

Eurydice (2009). Education on online safety in schools in Europe. Brussels: Education, Audiovisual and Culture Executive Agency.

GSMA (2007). European framework for safer mobile use by younger teenagers and children. Brussels: GSMA Europe.

Gunter, B. and McAleer, J. (1997). *Children and Television, 2nd Edition*. London: Routledge.

Hinduja, S. and Patchin, J. W. (2009). *Bullying beyond the schoolyard: preventing and responding to cyberbullying*. London: Corwin.

ITU (2009). Child online protection. Geneva: International Telecommunication Union.

Lenhart, A. (2009). Teens and sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging. Washington, D.C.: Pew Internet & American Life Project.

Lessig, L. (2006). *Code: version 2.0* (2nd ed.). New York: Basic Books.

Lievens, E. (2010). *Protecting children in the digital era: the use of alternative regulatory instruments*. Leiden: Martinus Nijhoff.

Livingstone, S. and Haddon, L. (Eds) (2009). *Kids online: Opportunities and risks for children*. Bristol: Policy Press.

Machill, M., Hart, T. and Kaltenhuser, B. (2002). Structural development of Internet self-regulation: Case study of the Internet Content Rating Association (ICRA). [DOI: 10.1108/14636690210453217]. *Info*, *4*(5), 39–55.

McLaughlin, S. (2007). Violent video games – Can self regulation work? *Communications Law: Journal of Computer Media and Telecommunications Law*, *12*(5), 157–67.

Mossberger, K., Tolbert, C. J. and McNeal, R. S. (2008). *Digital citizenship: the internet, society, and participation*. Boston, MA: MIT Press.

O'Neill, B. and Hagen, I. (2009). Media literacy. In Sonia Livingstone and L. Haddon (Eds), *Kids online: Opportunities and risks for children*. Bristol: Policy Press, pp. 229–39.

OECD (2011). *The protection of children online. Risks faced by children online and policies to protect them*. Paris: OECD Working Party on Information Security and Privacy.

OSCE (2010). Report of the OSCE representative on freedom of the media on Turkey and internet censorship. Vienna: Organization for Security and Co-operation in Europe.

Passey, D. (2011). Internet Safety in the Context of Developing: Aspects of Young People's Digital Citizenship. Lancaster: National Education Network Safeguarding Group.

Phillips, L. (2011, 16 March). EU to force social network sites to enhance privacy. *The Guardian*. Retrieved from http://www.guardian.co.uk/media/2011/mar/16/eu-social-network-sites-privacy

Ringrose, J., Gill, R., Livingstone, S. and Harvey, L. (2012). A qualitative study of children, young people and 'sexting'. London: NSPCC.

Ryan, J. (2010). Internet access controls: Three strikes 'graduated response' initiatives. Dublin: Institute of International and European Affairs.

Sacco, D. T. (2010). Sexting: Youth practices and legal implications. Boston, MA: Berkman Center for Internet and Society.

Safer Internet Programme (2009). *Awareness report on the status of online safety education in schools across Europe*. Luxembourg: European Commision, SIP.

Shariff, S. and Churchill, A. H. (2010). *Truths and myths of cyber-bullying: international perspectives on stakeholder responsibility and children's safety*. New York: Peter Lang.

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

UNICEF (2011). Child safety online – Global challenges and strategies. Florence: UNICEF Innocenti Research Centre.