2

Regulating Risks and Web 2.0 Technologies: Convergence, Technology and Social Policy

What do news stories of criminal prosecution of individuals involved in online paedophile rings, obligations on social networking services providers to address parental anxieties surrounding sexual predatory behaviour on network publics and the Summit on Bullying hosted by the White House have in common? A number of possible answers can be given to this question. One answer may be that it reflects our consciousness about the disorientating features of technology (Ohler, 2010: 77–90). The misuse of technologies taps into our

> primal forces that have been with us for thousands of years. These "forces of the cave," ... range from fearing predators, seeking food and shelter, and nurturing our children to protecting our mate and trusting fellow tribe members. (Dertouzos, 2001: 211)

Another answer might be that these are all responses to the way network infrastructures and information flows distribute risks. These incidents also illustrate how politicians, the mass media, law, industry and society construct and respond to these risks (Garland, 2003). The events do not of course tell us about growing societal preoccupation with enhancing the safety of children in the online environment or even what it is about Web 2.0 technologies and children's interaction with them that bothers us. Neither do they hint at the burdens increasingly shouldered by the State, child welfare organisations, law enforcement, parents and children in managing the security risks accompanying their risk-prone activities (e.g. emails, use of search engines and participation in network publics). The need to be seen to respond to risks in itself becomes a preoccupation of many parents and the communities in which they live. The US President's call for a community response in dealing with one pernicious threat faced by children is emblematic of a perennial dilemma for those living in a risk society. "Risks", as Ulrich Beck defines it, is a "systematic way of dealing with hazards and

J. Savirimuthu, *Online Child Safety*

insecurities induced and introduced by modernization itself" (1992a: 21). This chapter has two objectives. First, it seeks to explain and integrate the salient aspects in Beck's ideas about the risk society into online child safety discourse. In undertaking the task, an attempt will be made to identify how ideas of risk manifest themselves in the online child safety governance sphere of policymaking, rule development and discourse. Second, this chapter lays the foundation for the subsequent discussions on the standard setting role of law and the extension of its rules, values and norms to all stakeholders with the aim of creating a culture of safe and responsible use of Web 2.0 technologies and social media.

Living in the "risk society"

An overview

Beck identifies risk as a focal point in his study of the impact of the interaction between the State, industry and science on society in late modernity. In *Risk Society: Towards a New Modernity*, he offers us a grand theory, depicting the impact of techno-economic developments on society. He postulates that the risk society is a "catastrophic society" where "averting and managing" risks become norms rather than exceptions (Beck, 1992a: 24). In focusing on the concept of risk, Beck, unlike Marx or Weber, is not particularly interested in addressing the class and economic implications of the capitalist system of production (Lupton, 1999: 1–7). For him, the capitalist modes of wealth creation and distribution not only produce increased benefits and new opportunities for prosperity and development but they also generate negative or destructive outcomes – the logic of wealth creation, he suggests, sets in operation processes by which risks are not only created but they are also distributed to individuals across society. The ideological, technological, economic and political imperatives, which sustain the logic of wealth creation, produce risks that leave no part of society untouched. Beck concludes that advances in technology and science now pose society with a governance dilemma, since we can no longer be concerned

> exclusively with making nature useful, or with releasing mankind from traditional constraints, but also and essentially with problems resulting from techno-economic development itself. (Beck, 1992a: 19)

How society addresses this dilemma is in essence the "risk society" thesis and very much a part of the challenges confronted by the MSIG framework used to address online child safety issues. Indeed, it is a dilemma that confronts policymakers grappling with the services, products and activities that result from the convergence of networks, communications and information (OECD, 2004). The World Summit on the Information Society (WSIS), in its

Geneva Declaration of Principles, expressly regards the protection and preservation of children's right as an important priority in the development of information and communication technology (ICT) applications and operation of services (WSIS, 2003). Paragraph 90 of the *Tunis Agenda for the Information Society* states that the pursuit of economic growth through ICT should also incorporate "regulatory, self-regulatory, and other effective policies and frameworks to protect children and young people from abuse and exploitation through ICTs into national plans of action and e-strategies" (WSIS, 2005). The *Adolescent Declaration to End Sexual Exploitation* emphasises that without appropriate regulatory responses, the threats posed to children are likely to be endemic

> the continuing high level of sexual exploitation of children and adolescents in States in all regions, and at the increase in certain forms of sexual exploitation of children and adolescents, in particular through abuse of the Internet and new and developing technologies, and as a result of the increased mobility in travel and tourism. (WC III, 2008: paragraph 2)

A failure to respond to risks in a balanced and principled way has undoubted implications for the safety and well-being of individuals and trust generally. As the Organisation for Economic Cooperation and Development (OECD) noted in its policy document, trust is

> one of the central channels through which social identities are constructed in late modernity. Trust is fragile. Typically it is created rather slowly, but it can be destroyed in an instant by a single mishap or mistake. Once trust is lost, it can take a long time to rebuild. In some instances, lost trust may never be regained. (OECD, 2003)

Risks, reflexive modernisation and individualisation

The globalisation of risk with the resulting examination of the governance responses of the State and its institutions for wealth creation is a familiar trope in the discourse on modernity (Lupton, 1999; Beck, 1992a; Giddens, 1990). We will deal with the globalisation of risk in Chapter 6. For present purposes, we need to highlight two other insights from Beck's "risk society" thesis: the techno-economic advances which lead to the emergence of risks and individual and institutional preoccupation with redressing the uncertainty created by its pervasiveness in society (Jarvis, 2007; Giddens, 1991). The emphasis on techno-economic advances is central to Beck's vision of the "risk society" since it allows him to distinguish natural hazards from those categories of risks he regards as man-made (Beck, 1992a: 98). Man-made risks, he suggests, are generated by the logic of wealth creation, and these include pollution, unemployment, accidents in the work environment and breakdown in family and class structures. Sexual exploitation

and abuse of children is not a natural hazard but society's preoccupation with child safety issues can be treated as part of Beck's risk paradigm since the regulatory State continues to be one of the proponents in developing responsive regulatory systems (Hood *et al.*, 2001: 4). As Hood, Rothstein and Baldwin remark on the decision by the State to release paedophiles ex-offenders released from custody:

> What is new about this risk is the degree of recognition and public discussion it has attracted over recent decades ... [the] risks presented by released paedophile offenders are of high political and media salience across much of the developed world. Within the UK, that salience contrasts markedly with a lower, albeit growing, level of public attention and concern about child sexual abuse within the home by close family members. (Ibid., 2001: 41)

Faced with the generative nature of risks created by the logic of wealth creation, governments, institutions and individuals are faced with the prospect of being overcome by these negative consequences (ITU, 2009d). Beck argues that society in late modernity is unable to desist from establishing control and reducing the uncertainty that actual (or potential) risks create. However, it may be more accurate to say that government intervention here has to do with fostering public trust and confidence in demonstrating its ability to manage risks. We see Beck's ideas resonate, for example, in the security developments following the atrocities of the terrorists attacks in the United States and London, concerns about nanotechnologies, mad cow disease, severe acute respiratory syndrome (SARS), the anxieties revolving around the increasing sexualisation of young people and release of ex-sex offenders into the community (Wilkinson, 2001; Handmer *et al.*, 2007; Papadopoulos, 2010; Hood *et al.*, 2001: 41–2). Society's desire and need for certainty and control is manifest in the way governments now assume the role as managers of risk through the development of rules and mechanisms for identifying, monitoring and responding to a wide range of risks (Lofstedt, 2005). Individuals and institutions in society engage in what Beck terms as reflexive modernisation; society preoccupies itself with managing risks and becomes constantly dependent on mechanisms which lead to risks being audited, expert advice being sought when formulating policies and measures and regulations being designed to promote compliance with legal standards and obligations (ITU, 2010b; OECD, 2003). There are a number of examples even in the sphere of safeguarding children from commercial sexual exploitation that bring to mind the politicisation of risk and the process of reflexive modernisation taking place. For example, at the World Congress III against Sexual Exploitation of Children and Adolescents (WC III), it was noted that over 129 governments had adopted and ratified the Optional Protocol and an increasing number of

countries were ratifying the Child Prostitution and Child Pornography and the International Labour Organisation (ILO) Convention 182, the CPC Convention and Cybercrime Convention (WC III, 2008: paragraph 1). Additionally, a number of countries have prioritised online child safety issues in their national strategies, agendas and plans (ibid., 2008: paragraph 3). We can infer from the politicisation of risk the increasing role played by politicians and civil society in driving forward child safety agendas and risk-based modes of reasoning and policymaking activity (Beck, 1992a: 155–63). For Beck, these are the prime examples of risk becoming increasingly secularised and politicised. Risks (and their management) also become very much an important part of public consciousness, particularly as the media provides an increasingly influential avenue through which risks are defined and communicated to a wide audience. Unsurprisingly, in the area of online child safety, the media attention tends to be focused on the extreme edges of technological misuse or "worse-case scenarios" (e.g. online paedophile rings, suicide, self-harm, exposure to pornography and peer victimisation). Such is the anxiety that is generated that "we are left to wonder what else happens in the largely invisible world of the infosphere" (Ohler, 2010: 141). Managing risk in modernity becomes a reflexive process where the development of prudential and precautionary measures is seen as an ongoing process where the agency of political institutions becomes prominent in governance since

> questions of the development and employment of technologies (in the realms of nature, society and the personality) are being eclipsed by questions of the political and economic "management" of the risks of actually or potentially utilized technologies – discovering, administering, acknowledging, avoiding or concealing such hazards with respect to specially defined horizons of relevance. The promise of security grows with the risks and destruction and must be reaffirmed over and over again to an alert and critical public through cosmetic or real interventions in the techno-economic development. (Beck, 1992a: 19–20)

These last references to the "promise of security", the need for affirmation, and a public highly attuned to risks and the "cosmetic" nature of some of the interventions have a lasting impact on the sense in which "risk-based" regulation is understood: the distinction between actual and perceived risks becomes blurred and consequently contributes to society's continued anxiety about managing risks. Increasingly, the governance question is framed not in terms of whether online risks facing children should be regulated but what risk-based systems facilitate deliberative and participatory processes that enable the child safety policies and standards to be attained without compromising public trust (Graham, 2010: 244–5). The latter is particularly relevant as information networks and Web 2.0 technologies are seen

as producing risks and benefits that affect certain groups of individuals in society disproportionately. One reason for the "irrationality" of individual's responses to risks in society, sometimes characterised as "moral panics", is that techno-economic developments also transform structures and systems that have previously been regarded as frameworks for security and stability (i.e. welfare state, agrarian society, feudal structures). The transition from "industrial" to the "risk society" and the resulting loss in public trust and confidence in the State and its institutions is seen as leading to individuals assuming a greater role in managing their own safety and well-being (Beck, 1992a: 101; 1992b: 127–37). As Beck points out:

> Risk Society begins where tradition ends, when, in all spheres of life, we can no longer take traditional certainties for granted. The less we can rely on traditional securities, the more risks we have to negotiate. The more risks, the more decisions and choices we have to make. (Beck, 1998: 10)

The individualisation of risk subjects everyone in society to turbulence and social conflicts in varying degrees (Beck, 1992a: 134–5). The central point here is not that late modernity creates more risks, rather the changes wrought by technological advances create conditions, which lead to an individual's heightened awareness of risks and the quest for effective responses (Giddens, 1991: 123–4).

The emerging MSIG strategy

The International Telecommunication Union (ITU) in its 2009 Report highlighted the rapid penetration of ICTs across societies (ITU, 2009a). Individuals and organisations now have access to not only a range of information but also a wealth of computing applications. These developments have not escaped the attention of policymakers and governments. For example, under the *Digital Agenda for Europe*, electronic communications are seen as a necessary medium for creating a sustainable and inclusive economy (European Commission, 2010a). It is expected that broadband technology and online services will be made available to all Europeans by 2013 (European Commission, 2010b). Many homes now have access to online networks and the availability of multimedia services is now transforming the way information is accessed (ACMA, 2009a). Under Canada's Economic Action Plan, $225 million was provided to Industry Canada to increase broadband connectivity to areas not currently served (Government of Canada, 2011). The US National Broadband Plan views the networked economy as critical to improving domestic economic and social conditions and global competitiveness (FCC, 2011). The networked economy is seen as central to providing businesses, organisations and individuals with considerable opportunities, but these flows of networked information also bring with it vulnerabilities and threats that undermine trust and confidence

(Garland, 2003; Giddens, 1991). These threats and risks are not immediately identified since they exist in multiple communication platforms and in environments of collapsing national and international boundaries. The transition to a risk society also has important consequences for the way risks generated have now to be managed. For example, governments now have to assess, manage and regulate risks in society (Beck, 2002). Individuals in society, for example, are also vested with the responsibility for managing their affairs as traditional insurance and social infrastructures for maintaining cohesion are gradually loosened. The distinctive features of online safety risks are that the "producers", "managers" and "protesters" of risks are in effect the State, the ICT industry and, indirectly, educators and parents who make the products and services available to children (Van Asselt *et al.*, 2009: 360). This characterisation is important since many of the stakeholders assume an important role in the governance process and make decisions on the risk management strategies to be adopted. At the high level of regulatory theory a number of developments have taken place, which have undoubted implications for the way policymakers think about online child safety governance issues. In Canada, a policy document was produced to look at the effects of risk-based regulation (Government of Canada, 2004). Others have defined the risk-based governance in terms of the barriers to developing innovative regulatory responses. Policymakers in the European Commission highlighted the role of the precautionary principle as a touchstone for managing risks in conditions of uncertainty (European Commission, 2000). With children's increased exposure to Web 2.0 technologies, policymakers have also framed responsive risk governance in terms of worst-case scenarios – peer victimisation, children meeting sexual predators, exposure to illegal and age-inappropriate content and children accessing self-harm and suicide websites. These risks are understandably difficult to quantify and, consequently, provide the justification for pursuing reflexive regulatory strategies and measures. The reflexive responses underscore the heightened awareness of the scale and complexity of managing risks and anxiety and the need to ensure that risk management becomes an ongoing policymaking priority. There is concern that such anxieties, if left unchecked, may lead to overregulation or result in policymakers targeting individuals or organisations to assume responsibility for managing these risks (Sunstein, 2007). From a governance perspective, prioritising the regulatory agenda becomes a legitimate objective. For example, in response to the growing concerns about the impact of online security threats on user trust and confidence, the Australian government has undertaken a series of studies with the aim of identifying priority areas for risk management (ACMA, 2009c,d). Governments now regard encouraging parents and educators to supervise closely the activities of children aged 5–7 as a legitimate child safety objective (ITU, 2009b,c). Broadcasters, the Internet industry, Internet service providers (ISPs) and online service providers are encouraged to implement

design, technological and educational solutions (ITU, 2009d). Policymakers are provided with statistical indicators of risk-prone activities and risk-prone behaviours, which identify areas for regulatory activity and policymaking (ITU, 2009e). Consequently, we end up subscribing to the

> mean world syndrome [which] says that, because of the media's attraction to reporting the worst in human nature, people think the world is much more violent and dangerous than it actually is. It is certainly more dangerous than how most of us experience it. (Ohler, 2010: 143)

It follows from the preceding discussion that the resulting institutionalisation of risk now brings into the regulatory landscape non-State actors. ISPs, online service providers, mobile phone operators and NGOs are regarded as having important obligations and roles in online child safety governance (Klinke, 2009: 403–4). The Byron Report neatly encapsulates the significance of the individualisation of risks facing children by its three governance objectives:

> Reduce Availability – Reduce the availability of harmful and inappropriate content, the prevalence of harmful and inappropriate contact and the conduciveness of platforms to harmful and inappropriate conduct.
>
> Restrict Access – Equip children and their parents to effectively manage access to harmful and inappropriate content, avoid incidences of harmful and inappropriate contact and reduce harmful and inappropriate conduct.
>
> Increase Resilience – Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children. (Byron, 2008: 62)

Accordingly, as will be discussed in subsequent chapters, the responsibility for assessing and communicating risks will be directed at sector-specific industries (e.g. social networking sites, computer manufacturers, mobile phone providers, and ISPs). The gradual widening of the channels for risk management and allocation brings into the multi-stakeholder governance model a range of regulatory techniques for managing risks: private and public law, insurance and codes of practice. Even though Beck's thesis is not without its critics, his contribution, however, is important for our understanding of how and why risk-based regulation has become a defining characteristic in online child safety governance. We will examine some of the dynamics of risk-based governance systems in Chapter 7. The first matter to be considered is the extent to which the end-to-end design principle creates the techno-economic and social conditions that lead to

policymakers defining the roles and obligations of the stakeholders within the MSIG framework.

Children, Web 2.0 technologies and social media

Even though this is not a book about the protocols and architecture of the Internet, some appreciation of its function and design principles is necessary if we are to begin to understand the relationship between the logic of information flows, the new channels for risk distribution and anxieties about children's safety and well-being and the attainment of the three governance objectives. To this end, the discussion will address three aspects in turn: the design and architecture of communication technologies, convergence between youth culture and technology and the policy implications arising from the interaction between the technical infrastructure and design, online security threats and risks and governance challenges.

Design principles and the architecture of the Internet

The Internet is first and foremost a complex network of computers. The original designers of the Internet were not concerned with providing virtual worlds, social networking sites, web streaming or email services (Castells, 1997). Their challenge was to develop protocols that allowed networks to connect with each other (Berners-Lee *et al*., 2000). As Werbach makes clear:

> Unlike traditional communications networks, the Internet does not provide a particular kind of service. Its designers set out not to deliver content, but to interconnect networks (hence the name Inter-net). Neither services offered nor physical infrastructure nor geographic location determine whether something is part of the Internet. (2002: 47)

This extract highlights two particular aspects with regard to the interaction between the architecture of the Internet and its design principles. First, the design principles and architecture can be likened to providing engineers and programmers with tools and a medium through which information can be disseminated across networks and represented as text, images and sound. The fundamental design principles shaping much of the work undertaken by these individuals in creating a technical communications infrastructure were those of interoperability, decentralisation and non-discrimination – the information space was to be an environment that was capable of being accessed by anyone, from any country and from any computer or communication device (Berners-Lee, 2000: 37; Table 2.1). As we will discover later, the technological affordances and the channels through which information flows can now be accessed owe much to the priority given to design rather than security principles (Dertouzos, 2001: 209). Security principles, like those relating to confidentiality, integrity, authenticity and availability,

Table 2.1 Tim Berners-Lee design principles for the World Wide Web

An information system must be able to record random associations between any arbitrary objects
If two sets of users started to use the system independently, to make a link from one system to another should be an incremental effort, not requiring unscalable operations such as the merging of link databases
Any attempt to constrain users as a whole to the use of particular languages or operating systems was always doomed to failure
Information must be available on all platforms, including future ones
Any attempt to constrain the mental model users have of data into a given pattern was always doomed to failure
If information within an organization is to be accurately represented in the system, entering or correcting it must be trivial for the person directly knowledgeable

Source: http://www.w3.org/People/Berners-Lee/1996/ppf.html.

are concerned with managing the flow of information so that the right information is made available to the right persons, at the right time and at the right place (OECD, 2002a).

The design principles are reflected in the "protocols" now used by online intermediaries and mobile phone companies to provide users with opportunities to exchange information, and view or experience social media on a variety of platforms (Lane, 2008). "Protocols" are rules, which enable networks to connect with each other. The Internet is in essence based on a number of protocols known as the Transmission Control Protocol/Internet Protocol (TCP/IP). Accordingly, the adoption of protocols enables files to be transferred, emails to be sent and information in all forms to be stored and disseminated. The TCP/IP protocols can be categorised into four functional groups or layers, which enable users to exchange content over networks (Table 2.2). These relate to Content, Application, Transport, Internet protocol, Link and Physical properties like cables and wires (Solum *et al*., 2004).

Second, many of the innovations and developments that we see today (i.e. Smartphone, portable media devices and multimedia communication platforms) can be traced back to the design principles and the architecture of the Internet (OECD, 2008a). The development of software applications and ready availability of broadband connectivity has contributed greatly to the emergence of a vibrant communication ecosystem (ITU, 2009a; OECD, 2010a). P2P file-sharing technologies, voice over Internet protocols (VOIP), wireless connectivity, mobile applications, cloud computing and next generation mobile phones enhance economic and social activities by enabling individuals and organisations to access, create, store and distribute information. Social networking sites like Facebook, Bebo and MySpace enable

Table 2.2 The layer principles

Application layer
There are user protocols aimed at providing users with online services.
Examples include services for remote login (Telnet), transfer of files (FTP), sending email (SMTP) and exchange of information between a web client and web server through HyperText Transfer Protocols (HTTP)
Other examples of applications include voice over internet protocols, P2P file-sharing applications and web browsers (e.g. Firefox and Internet Explorer)
There are support protocols which address system functions
Transport layer
This layer provides end-to-end communication services for applications.
The Transmission Control Protocol (TCP) provides a connection-oriented transport service
The User Datagram Protocol (UDP)
Internet layer
The Internet Protocol (IP) enables any set of hosts to exchange data packets
Internet Protocol version 4 (IPv4)
Internet Protocol version 6 (IPv6)
Internet Protocol Security (IPsec)
Link layer
A link layer protocol enables communications on directly connected networks. For example, organisations may have local area networks which implement standards like Ethernet

Source: RFC 1122, Available at http://datatracker.ietf.org/doc/rfc1122.

information to be freely accessed, exchanged and created. It is hard not to notice that at the core of the Internet and the evolution of Web 2.0 technologies is the belief that innovation, creativity and freedom of expression thrive best in an environment of free markets, entrepreneurial endeavour and minimal State intervention (Benkler, 2006). As Zittrain recalls:

> From its start, the Internet was oriented differently from the proprietary networks and their ethos of bundling and control. Its goals were in some ways more modest. The point of building the network was not to offer a particular set of information or services like news or weather to customers, for which the network was necessary but incidental. Rather, it was to connect anyone on the network to anyone else. It was up to the people connected to figure out why they wanted to be in touch in the first place; the network would simply carry data between the two points. (2008: 27)

It is not an exaggeration to say that without the four functional layers and its underpinning design principles, we would not have seen the acceleration of a networked society comprising online intermediaries, network operators and commercial product manufacturers (OECD, 2010a). Neither, it should be said, would the absence of the functional layers have created the necessary incentive structures for the ICT industry, online services providers and mobile operators to make available products and services which mirrored consumers' need for immediacy, intimacy, community and information (Lane, 2008: 5–7).

The advances in communication technologies and the ubiquity of computing represent an important paradigm shift in the way the logic of sustaining information flows frames economic, technological and cultural activity (Castells *et al*., 2007). Mobile phones, for example, now come packaged with software applications, widgets, and Wireless Application Protocol (WAP) that have standard web technology components to enable users to engage with the others in online environment (Lane, 2008). One study forecasts not only the growth of mobile social networks but it is also expected that this trend will culminate in transforming the way individuals in society will interact and communicate (ibid., 2008: 15). The OECD Working Party on Telecommunication and Information Services Policy observed that "[c]onvergence in electronic communications is bringing together industries in the communications area which were previously viewed as separate in both a commercial and technological sense, and which have quite distinct regulatory traditions and arrangements" (OECD, 2004: 5).

Convergence in broadcasting, telecommunication and entertainment impacts a wide range of economic and social activities. Consequently, governments and regulators continue to be alert to the public interest issues raised by the ubiquitous computing environment (Schewick, 2010: 20–2, 37–8). Many child safety issues are increasingly linked to the governance implications arising from the ICT industry and online services providers leveraging the capabilities of networks and telecommunications. Children's consumption of new technologies now provides a catalyst for a whole range of technical issues confronting online intermediaries, the Internet Engineering Task Force and the World Wide Web Consortium (W3C) (WGIG, 2005). From a child protection perspective, the interaction between children's consumption habits and the individualisation of risks has also led to a re-examination of how risks can be better managed by the ICT industry and related online service providers (WSIS, 2003). With the convergence of the broadcasting and telecommunication sectors, and the emergence of new online services providers, risk-based regulation efforts continue to be directed at promoting sector-specific assessments, standard setting initiatives and improving compliance (ITU, 2009d; WSIS, 2005). This process of reflexive modernisation is depicted in the technical literature as the end-to-end arguments. In a highly influential paper written in the early 1980s,

the question of how applications should be incorporated into the technical infrastructure of the Internet was addressed, with the recommendation that the application-level functions be built into the high levels, rather than the lower levels of the system on the basis that

> the function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end-points of the communications system. Therefore, providing that questioned function as a feature of the communications systems itself is not possible. (Saltzer *et al.*, 1984: 278)

The allocation of specific applications and services away from the core of the system were seen as reducing the demands on the lower-level system and ensuring efficiency, reliability and flexibility gains (Blumenthal *et al.*, 2001: 71). Despite the seeming elegance and simplicity of the end-to-end argument, the premise is clear: the logic of information flows is seen as requiring, if not compelling, the end points (i.e. those who make the technology to be consumed, those who make consumption of online services and technology possible and those who consume the technology and services) to assume ultimate responsibility for managing and allocating responsibility for risks. For example, under the end-to-end principle, the architecture of the Internet in effect vests the responsibility for managing risks, to varying degrees, with the various participants in the information chain. Recall that the applications are situated at the core of the Internet's technical infrastructure, and, consequently, the functional layers do not discriminate as to the type of content being sent and neither do the information flows make the characteristics of the senders and recipients immediately discernible to end users. The end-to-end principle, as originally formulated, can also be seen as reflecting an ideological preference for limited State intervention, with market rules and norms being seen as appropriate instruments for regulating the telecommunications and broadcasting industry. The debates that we now witness in online child safety governance regarding the role of online intermediaries involves, in essence, an argument about how the negative consequences of information flows are to be managed by the existing framework for regulating telecommunication services across network infrastructures and content that can be accessed from these platforms. For example, mobile phones and Smartphones now incorporate a bundle of software applications into their hardware. The aim of these measures is to provide consumers with a wide range of services and access opportunities. With these benefits, and mindful of the end-to-end principle, mobile and online content service providers are now vested with the responsibility of ensuring that the information accessed through their products and services correspond with national content standards and policies (ITU, 2009d). The end-to-end principle also confronts policymakers

with difficult choices regarding the outcomes of managing the uncertain nature of convergence, the speed and scale of convergence and the individualisation of risks (OECD, 2004:14). Risks in short are now socialised and engender a continued process of reflexive modernisation as part of the MSIG strategies in the area of regulatory policy, national coordination and legislative activity (ITU, 2009e).

The digital natives' landscape

The exponential growth of the Internet is transforming the way individuals, and in particular children, now interact with communication technologies and social media (Negroponte, 1995: 200–2). Commentators like Livingstone and Bovill have remarked on the significance of the growing convergence between youth culture and technology (Livingstone, 2003b; Bovill *et al*., 2001). These technologies have become an integral part of children's daily lives and activities (ACMA, 2009b; Ipsos Mori, 2009). The European Commission's *Safer Internet Plus Programme* has funded projects examining the online experiences of children from 21 Member States (European Commission, 2011b: 9). The EU Barometer Surveys in 2005 and 2008 showed that in 2005, 70 per cent of 6- to 17-year-olds in the countries were using the Internet (Eurobarometer, 2005, 2008). By 2008, this number had increased to 75 per cent, with the finding that 60 per cent of children aged between 6 and 10 years were online. Another view of convergence is that communication technologies now enable individuals to interact with each other without the traditional constraints of time, distance and space. Ubiquitous and mobile computing now free individuals from the traditional physical constraints associated with interaction and consumption of social media (Castells *et al*., 2007: 127–46). As Ito remarks, technological affordances allow children to take full advantage of participating in network publics and negotiate their identities (Ito *et al*., 2008). Children aged 5 to 12 years not only spend an increasing amount of their leisure activity online but they also use a range of media platforms to access information, play games and interact with their peers (Staksrud *et al*., 2010). The Office of Communications (OfCom) noted that during the past five years there has been a gradual transformation in the way young children interact with social media and technology (OfCom, 2009). Growing interoperability at the application or device levels and the consolidation of telecommunications, media and entertainment have contributed to this shift in children's engagement with technology and their environment. Similar trends have been noted in developed economies outside the EU, including America, Canada and Australia. In the *Digital Futures Report 2010*, consumption of the Internet and communication technologies by Americans was shown to increase as the age decreased (Centre for Digital Futures, 2010). In an extensive study examining the online behaviours of children (grades 4 to 11) in Canada, between 2003 and 2005, communication

technologies were found to be well and firmly embedded in children's daily lives:

> Young people, on the other hand, do not see the Net as a distinct entity or environment. It is simply one more space in which they live their lives – connecting with friends, pursuing interests, figuring out what it means to be a teenager and a grown up. (Media-Awareness, 2005)

The Australian Bureau of Statistics (ABS) identified similar trends in its study *Children's Participation in Cultural and Leisure Activities* (ABS, 2009). It was found that Internet use and frequency of use also increased with age. For example, during April 2008–09, 96 per cent of young adolescents (aged 12–14) accessed the Internet, in contrast to only 60 per cent of five- to eight-year-olds; Internet access was now available to children at home, school and elsewhere (79 per cent), and the activities for which the Internet were used included education (85 per cent), playing online games (69 per cent) and downloading music (47 per cent).

Design, cultural convergence and the genres of participation

What is "cultural convergence"?

Terms like the "digital generation", "mobile youth" and "digital natives" form very much a part of popular discourse on children and their interaction with new technologies (Rideout *et al*., 2007). In essence, these terms attempt to capture a radical transformation in children's interaction with their environments in contemporary society (Prout, 2005; James *et al*., 1998). At a basic level, "convergence" in the age of mobile computing can be viewed as the coming together of information, media and communication. Convergence can also be viewed more expansively (Jenkins, 2006). As many commentators have pointed out, Web 2.0 technologies are imbued with social and cultural meanings (Benkler, 2006). According to Jenkins, convergence

> represents a paradigm shift – a move from medium-specific content toward content that flows across multiple media channels, toward the increased interdependence of communications systems, toward multiple ways of accessing media content, and toward ever more complex relations between top-down corporate media and bottom-up participatory culture. (2006: 243)

Jenkins' description frames the discourse on network publics and technological affordances well. There is of course a "qualitative change in users' experience of everyday life ... [which results in a] ... technosocial sensibility" (Castells *et al*., 2007: 141). Cultural convergence can also be represented in

another way. Benkler observes that participatory cultures deviate from the norm of hierarchical and centralised models for coordinating interactions and a key aspect of this improvement

> has been the technical–organizational shift from an information environment dominated by commercial mass media on a one-to-many model, which does not foster group interaction among viewers, to an information environment that both technically and as a matter of social practice enables user-centric, group-based active cooperation platforms of the kind that typify the networked information economy. (Benkler, 2006: 357)

Childhood in 2012 is lived in spaces created by information networks. Children's use of mobile phones, the meanings attributed to the building of extensive "friend" lists and the use of social network profiles as tools for self-presentation and admission into online communities are manifestations of what life in a networked society means for individuals, particularly children (ibid., 356–8). The role of Web 2.0 technologies in enhancing children's autonomy has also marked an important shift in what Senft describes as a growing culture of gossip, self-branding and sexual display as leitmotifs of children's fascination with new technologies, social media and celebrity culture (Senft, 2008). Cultural convergence also shapes the way children engage and participate in these environments – not as passive actors but as autonomous individuals with their own identities, preferences and values (Herring, 2008: 71–92). There is perhaps a sense of a new sociability where children now exercise their newfound autonomy through "consumerism, faddish trends, cultural identity, peer-group formations, relationship with existing social institutions" (Castells *et al*., 2007: 142) Creative uses of technologies have been used to promote civic participation and critical media literacy skills (Goldman *et al*., 2008: 185–206). Mobile phones now embed these preferences and tastes so as to enable children to enjoy and experience a range of social and cultural opportunities. A study, focusing on the lives of children aged between 8 and 18, found that ownership of mobile phones and Smartphones amongst this group of consumers is on the rise (Rideout *et al*., 2010). For many children, mobile phones open up opportunities for engaging with their communities, participating in support networks, and entertainment (Ling, 2008: 43, 58, 77). Teenagers use mobile phones for texting, taking pictures and accessing online content. "Cultural convergence", according to Stald, has elevated the wisdom of peer participatory cultures and norms:

> Because of the always there, always on status of the mobile and the pace of exchange of information, and because the mobile is the key personal communication device for so many young people, it becomes important

> in establishing social norms and rules and in testing one's own position in relation to the peer group. (Stald, 2008: 143–64)

Her findings correspond very much with the ongoing work by Ling on mobile phone use. In his research, Ling rejects any suggestion that mobile phone use is "exceptional" or novel; rather, he sees the mobile phone as a tool through which ritual social interactions and social bonding take place (Ling, 2008). Communication technologies are instruments for expression, cultural interaction and identity experimentation (Stern, 2007). In her study involving the use of communication technologies by adolescent girls, Stern noted that IM tools were not simply tools for transmitting information or content but that they were also utilised to create communities and establish norms of behaviour. There is also a sense, in reviewing the studies from the Kaiser Family Foundation and the Pew Internet & American Life, that young children view interactive technologies as private communication spheres where intrusions by parents and other persons are kept to a minimum (Rideout *et al*., 2010; Lenhart *et al*., 2008). Social networking, regardless of whether it takes place on a mobile phone or personal computer, is the digital equivalent where children

> hang out, jockey for social status, work through how to present themselves, and take risks that will help them to assess the boundaries of the social world. They do so because they seek access to adult society. Their participation is deeply rooted in their desire to engage publicly. (boyd, 2007: 137)

Finally, convergence allows individuals to engage with information, content and users anytime and anywhere – the de-centralisation of networks of communication infrastructure also creates new spaces for communication and interaction (and one which as a consequence erodes the dominant roles of parents and educators and leads to the blurring of the boundaries between childhood and adulthood).

Convergence, participatory cultures and genres of participation

Convergence can also be said to represent a cultural phenomenon comprising not only of participation but also a whole range of activities, which include interaction, formation of relationships, identity expression, community support, and engagement in creative activities (Livingstone, 2005a; Table 2.3).

Discussion forums, IM and social networking sites now provide children with opportunities to form communities and engage with their peers and persons they meet online (Livingstone, 2008b). Many social networking sites have taken advantage of the design and architectural principles to create innovative features on their platforms, by incorporating video, chat and IM facilities. Identity expression, experimentation and peer acceptance are

Table 2.3 Participatory cultures and genres of participation

	MMORPG/virtual worlds	**Blogs**	**SNS**	**Chat/IM/ mobile**
Content – *child as recipient*	Identity media literacy and strategic thinking	Identity media literacy	Identity media literacy, writing skills and creativity	Identity media literacy and strategic thinking
Contact – *child as participant*	Social communication	Building communities and relationships	Relationships and social interaction	Social interaction/ collaboration
Conduct – child as actor	Citizenship Skills and values	Support peers	Social communication content	Citizenship Skills and values

Source: drawing on AMF, 2009 and EU Kids Online, 2009

very much in evidence in the way children use these sites to interact with each other. Disclosure of information is regarded as part of the process of gaining access to online communities and interacting with others. For example, social network sites allow users opportunities to disclose a range of personal information – identity, age, gender, and address. The decision to disclose personal information like screen names, preferences and contact details may be based on a number of factors: the perception of relative safety of the online communication platform, opportunities to make friends and share similar interests, identity experimentation, anonymity, the accessibility of tools for managing risks and the absence of parents and educators in these communication spaces (Lenhart and Madden, 2007c). Social networking sites also fulfil the need of users to define their communities and to be connected with others. Consequently, search directory services provide individuals with opportunities to seek out friends and lifestyle interests. Identity and sexual experimentation is also very much a part of the network sociability, and the transition from adolescence into adulthood. To some children, the anonymised and disintermediated environment provides them with an opportunity to experiment with different persona and lifestyle experiences. Others use the online environment to seek assistance and support from their peers (Livingstone *et al.*, 2011). Whilst chat and IM create invaluable spaces for social interaction and learning, the Youth Internet Safety Survey 2 reported that children were also using communication platforms and tools to assert their autonomy and identity by engaging in discussions about sexual preferences and lifestyles (Mitchell *et al.*, 2007c).

This overview of the rich participatory culture, which defines childhood in the networked society, contains three important lessons for risk-based

governance. First, the very same activities, which are celebrated by Web 2.0 enthusiasts, are regarded as potentially risk-prone activities, even though these may not be readily quantifiable (Asselt *et al.*, 2006). Second, the framing of the "risk-prone" behaviour will inform online child safety governance policymaking and strategies (Mitchell *et al.*, 2007a,b). Third, social constructions of childhood will influence the expansion of the precautionary principle to address not only risks but the resulting "uncertainties" surrounding children's risk-prone behaviour, and perhaps confirm the politicised nature of online child safety governance (James *et al.*, 1997). The latter is of particular relevance as politicians and law enforcement may respond to public concerns about the effects of particular harms and risks by seeking the private sector to communicate and justify their risk management strategies and responses.

It may be useful to spend some time reflecting on how Web 2.0 technologies and affordances lead to businesses and industry becoming "risk producers" and agents in the distribution and individualisation of risk (Van Asselt *et al.*, 2009: 359–60; Table 2.4). In a highly competitive environment, the business models of social network providers like Twitter, Facebook and MySpace and the mobile phone industry recognise the value of innovation. Online service providers and manufacturers of new technologies align their services with the needs of their users. For example, mobile phone operators

Table 2.4 Technological affordances and network publics

Category	Description	Features which are most frequently used	Text	Photo	Video	App
Friending	Forming communities and making friends, sharing interests, and lifestyles	Profile pages, search directory, linking to social media, interactive communication and browsing	Post View	Post View	Post View	
Identity lifestyle	Experimentation, Sharing offline/online experiences friendships, risk taking, creativity, exhibitionism	Games, rating, browsing, use of social and interactive media, updating of profiles, extending friendship circles, gossip, alert features	Post View			

Source: Adapted from Lane, 2008: 10.

now ensure that their services and devices "avoid overcrowding or creating overly complex user interfaces" (Lane *et al*., 2008).

Mobile phones continue to be packaged with software applications which, allow users to send SMS texts and take photographs with ease. Virtual worlds have become popular online environments for many children. These are applications that leverage the architecture of the Internet and provide users with an online environment. Users of these applications can interact with each other through a persona, known as avatars, and communicate through the use of text and icons. Virtual worlds have also expanded to provide users with entertainment and games, which can involve a large number of players not confined to any particular geographical locality. In a recent report it was stated that more than $1.38 billion was invested in 87 virtual goods-related companies. According to the Virtual World Management (now Engage Digital Media), there are over 200 youth-oriented virtual worlds (which includes those which are planned or in active development).[1] The figures show an increase, when compared with 150 virtual worlds in 2008. The growth area appears to be in the market for children with three sub-categories representing the age groups 7 and below, 8 to 12 and 13 and above. Some examples of virtual worlds for children include Club Penguin, Webkinz, Barbie Girls, Moshi Monsters, Lego Universe and Adventure Rock. The demographics of these sites suggest that the reasons children access these sites are not dissimilar to those we have seen in other mobile social networking environments (Lim *et al*., 2010). Children are provided with tools to enable them to participate in communities, share interests and make friends, develop their identity and create user-generated content (Jackson *et al*., 2009; Marsh, 2010).

In summary, the logic of network infrastructures and information flows illustrate the democratic, developmental and social opportunities that Web 2.0 technologies make possible. These are evident in three areas. First, technological affordances create new spaces for communication. Second, communication tools are imbued with social and cultural meaning and these are reflected in the way users negotiate social norms, relationships and their individual identities. Finally, children can exercise their newfound autonomy, which may not be hindered or governed by parental rules and norms. Integrity, reliability and authenticity are assumed to be the necessary pre-requisites for engagement, affirmation and self-validation. Web 2.0 technologies provide society, and children in particular, greater choices and opportunities. More significantly, in the light of Beck's risk society, the expanding networked society now has in place the necessary conditions, which enable risks to be distributed, communicated and individualised. Individualisation also brings with it a heightened awareness of the risks that are generated from engagement with digital content and network publics. More importantly, as children now discover their newfound autonomy, it is important to note that they still continue to engage in these activities within a patriarchal society, which considers them to be vulnerable, risk-

prone and which, crucially, defines the rules within which these freedoms are to be enjoyed (Castells *et al*., 2007: 146–7). In the next section we will identify the different dimensions of risks, how these are related to Web 2.0 technologies and its implications for child protection policymaking.

Online child safety: The individualisation of risks, reflexive modernisation and insecurity

The unexceptional nature of online child safety

Palfrey and Gasser stress that the online environment does not raise any novel safety or child protection issues – indeed, they argue that parents' and educators' perceptions of the online environment as being more dangerous could be attributed to their lack of familiarity with the Internet infrastructure and communication technologies (Palfrey *et al*., 2008). Whilst not averse to informed parenting and rule making, the authors stress that many of the online risks and threats have their offline equivalents and the root causes for contact and conduct risks are "poor judgment, a lack of concern for the well-being of others, human depravity, mental illness, and so forth" (ibid., 2008: 98).

Policymakers are, however, confronted with an unenviable conundrum when faced with assertions like these (ITU, 2010). Regulating the communications and broadcasting industry is challenging at the best of times, given the volume and reach of many of the risk-prone activities (e.g. email, SMS text, online gaming, social networking) that make children particularly susceptible to online threats. Risk-prone activities include not only the amount of time children spend online but also those risks which emerge from their engagement with technological affordances and social media (Lenhart, 2007). The ABS in its 2009 Children's Participation in Cultural and Leisure Activities (CPCLA) Survey reported that 2.7 million children aged 5 to 14 years (7 per cent) used the Internet (ABS, 2009). Their online activities included educational activities (85 per cent) and playing online games (69 per cent). These activities are also related to their exposure to online risks or suggestive of their tendency to engage in risky online behaviours. In this same study, an estimated 3 per cent of children who accessed the Internet reported experiencing online safety incidents (e.g. approximately 72,000 children). Three per cent of children who have mobile phones (28,000 children) reported similar negative experiences. Sixty-five per cent of teenagers have been contacted by online users not in their peer group (Lenhart *et al*., 2007a: 35), and 31 per cent have "friends" whom they have never met, 34 per cent use the sites to make new friends (ibid., 2007a: 32), 4 per cent of mobile-owning children from the age of 12–17 have sent provocative or nude images of themselves via SMS text (Lenhart, 2009: 5) and 13 per cent of teens have received threatening or aggressive email, instant message or text messages (Lenhart *et al*., 2007b: 3). The Eurobarometer 2007 Survey also reported similar experiences by children in the age groups

9–10 and 12–14 (Eurobarometer, 2007). Online child safety governance has to address the child protection issues emerging from children as users/consumers and the risks generated by misuse of network infrastructure and communication technologies (Brenner, 2010). The online environment creates incentives for behaviour that we ordinarily would not encounter in the offline environment. Yar points to the exceptional nature of the "social interactional features of the cyberspace environment" which contributes to the growth of illegal activity and vulnerabilities (2006: 12). This is perhaps misconceived. At best, the online environment can be seen to raise intractable problems of policing and enforcing domestic laws and regulations (Brenner, 2010, 163–76). What perhaps distinguishes networked communications and information flows from their real space equivalents are the speed, scale and frequency with which deviant criminal activity can be perpetrated and the compliance issues they generate for national legal systems. However, it should be said that even though the risks are unexceptional, they are essentially invisible and their materialisation uncertain (Van Asselt *et al.*, 2009: 360–1). How we identify, assess and respond to risks is a perennial problem for designing effective risk-based regulation processes. The significance of the rhetoric of "safety" and its relationship with Beck's "risk society" is explored more fully below.

The logic of information flows and the individualisation of risks

Digital spaces are now seen as threats to children's safety and well-being. Network structures and information flows provide a new context where society becomes preoccupied with managing risks. Mobile phones and social networks are regarded as tools for victimising peers, chat rooms can now be misused by adults to solicit minors and P2P software programmes enable individuals to seek out illegal content stored on networked repositories with a global reach. Web 2.0 technologies are regarded by organised criminal gangs as enabling them to undertake their activities without detection by law enforcement (Tarissan *et al.*, 2009). Often, this can be done across transnational borders and without regulatory oversight (GAO, 2003). As noted previously, communication networks now create multiple opportunities for misuse and numerous access points through which children can be exposed to harm. Not only can a child be exploited through a number of access points (e.g. mobile phones, email, IM, virtual worlds, online games and social networking sites) but the abuse or exploitation of a child victim can also be relayed live to other observers for their sexual gratification or the impact can be significantly intensified by making the content or incident accessible to everyone with an Internet access (e.g. sexting and cyberbullying). It is this sheer complexity of the networks of information flows and the problems of managing risks and uncertainty that exacerbates the problems of policing and the difficulties faced in securing compliance with national laws and rules. Information flows are seen as contributing to the growing feeling

that the networked society generates risks that cannot be easily managed and controlled. Some continue to view the characteristics of networks and information as *the* cause of social disorder and uncertainty "reminiscent of the wild, wild West" (Chisholm, 2006: 75) Policymakers have responded to the growing anxiety by adopting managerial strategies like identifying the "risk categories" as well as the activities that expose children to unacceptable risks to their safety and well-being. Accordingly, studies have been undertaken to help inform policymakers, law enforcement, parents and educators about the relationship between children's online activities and incidents encountered in these environments. Managing risk and uncertainty involves a process of generating surveys, studies, reports and research. The EU Kids Online Project is an apt example of one reflexive modernisation activity where empirical surveys and studies are regarded as an appropriate basis for promoting informed decision-making and formulation of policies (Table 2.5).

Even as a general overview of the nature of the online child safety governance challenge, this taxonomy provides us with a snapshot of Beck's risk society – risk, reflexive modernisation and individualisation of risks. It also illustrates a potential dilemma for governance strategy since a scientific appraisal of the risks is not readily possible as the likely materialisation of the harm is uncertain until a series of causal behaviours are engaged in. For example, faced with media and law enforcement reports of the threats posed by online sexual predators, policymakers take the view that the potential risk under conditions of uncertainty must be avoided by implementing rules and precautionary norms (e.g. privacy rules, filtering software, parental control rules and children being encouraged not to speak with strangers). The

Table 2.5 Online child safety incidents

	Commercial	**Aggressive**	**Sexual**	**Values**
Content – *child as recipient*	Advertising, spam and sponsorship	Violence, hate, racist	Pornography, child sexual abuse and exploitation	Hate, biased or misleading advice
Contact – *child as participant*	Profiling, data mining	Victimisation by peers	Online sexual solicitation	Inappropriate lifestyle choices
Conduct – child as actor	Gambling, computer misuse, illegal downloading	Victimising peers	User generated sexual content	Participant in lifestyle communities (i.e. bulimia, self-harm and anorexia)

(Source: Adapted from EU Kids Online – Hasebrink *et al.*, 2009.

globalisation of risk-based regulation is also evident in the reflexive processes in play in countries like Australia, Canada, the United States and Member States in the EU, who have also undertaken similar mapping exercises with the aim of grounding their responses in empirical work. The focus of the child protection surveys is frequently directed at the relationship between children's access to the Internet and the likelihood of their increased exposure to online risks (Livingstone and Haddon, 2009b; AMF, 2009; Eurobarometer, 2006). In Canada a comprehensive study was conducted seeking to identify the attitudes, expectations and practices of children and young Canadians regarding their use of the Internet (Media Awareness, 2005). The study – *Young Canadians in a Wired World Phase II, Trends and Recommendations* – confirms the growing consensus amongst researchers and policymakers across the world that as the Internet and communication technologies become an integral part of children's lives, there will be an increase in their exposure and potential vulnerability to online safety incidents (2005: 5). The study also revealed that children (grades 8 and 9) encountered a number of sites with violent (28 per cent) or sexually inappropriate (32 per cent) content (2005: 17). Children, in this study, indicated that they did not actively search for websites with adult chat (91 per cent), only 16 per cent admitted searching for pornography, and boys were more likely than girls to seek out sites with violent or offensive content (2005: 18). These findings from Canada also correspond very much with the findings made by the Kaiser Family Foundation's *Generation M2* regarding children's media consumption habits (Rideout *et al*., 2010; OSTWG, 2010; ACMA, 2010a). In its studies of media consumption habits and trends amongst children and their families, the Australian Communications and Media Authority (ACMA) noted the close correspondence between media penetration in society and children's increased exposure to online safety risks (ACMA, 2010a). The findings also provide a context for thinking about the governance options and the nature of the measures to be adopted within the MSIG framework. A brief account of the three risks, which are mediated through networks and information flows will now be provided, and these are online sexual solicitation, illegal and inappropriate content and peer victimisation.

Online sexual solicitation

Web 2.0 technologies provide individuals with new avenues through which children can be targeted and lured into sexual activity without detection by parents or educators. Crucially, in online sexual solicitations, the offender aims to develop a foundation of trust with the child victim (CEOP, 2010a). Olsen observes that individuals targeting potential victims aim to identify

> three categories of characteristics that make them particularly vulnerable to a predator's lure: personality traits and emotional traits, behavioral patterns, and dysfunctional family dynamics. (Olson, 2007: 238)

Olsen is quick to add that the existence of these characteristics does not invariably lead to a meeting or abuse. The problems in establishing the identity of online participants and the ease with which some adults have used social engineering techniques to solicit minors for sexual activity have raised concerns about the security of these communication platforms for children. For example, in *R v Newman* (2010), the offender set up false identities in chat rooms accessed by young people with the aim of identifying prospective victims. In *R v Asplund* (2010), the offender had at his disposal a wide range of communication tools (e.g. mobile phones, SMS text messages and the Internet)

> to feed into and gratify his sexual titillation and fantasies with a long term view of having her submit to sexual activity with him ... demonstrated by his use of the Internet to persuade her to send him photos of a highly intimate and sexual nature, by his access to resources to shower her with money and bombard her with communications, by his toying and manipulative Internet exchanges earlier referred to. (2010: paragraph 7)

Apart from the risk of children meeting their online contacts "face-to-face", it is also becoming apparent that a number of offenders use chat rooms and IM to engage in discussions with children about sexual matters as a way of self-gratification and grooming a child for non-contact sexual activity. These "hit and run" tactics have been particularly noticeable with the emergence of webcams. Online sexual solicitation can be broadly understood as the process by which a sender aims to procure a child to engage in sexual activity or other forms of sexual gratification. This can include flirtation as well as more explicit forms of sexual activity (McQuade *et al*., 2008). Online sexual solicitation is one of the major parental concerns and source of anxiety and distress. In Australia, over 47 per cent of the parents in a survey expressed fears about their children talking to strangers (ACMA, 2009b: 75). In a recent study, it was pointed out that children received most online sexual solicitations from their peers or individuals from the age groups of 18 and 21 (ISTTF, 2008:14). The Child Exploitation and Online Protection Centre (CEOP) highlighted a rise in reports about grooming activity in online environments frequented by children (CEOP, 2009). The report notes that CEOP investigations increased from 20 per cent in 2006/7, 40 per cent in 2007/8 to 48 per cent in 2008/9 (CEOP, 2009: 8–12). It is also apparent, as the study conducted at the Crimes against Children's Research Centre points out, that one in five minors tend to be solicited online (Finkelhor *et al*., 2000; Wolak *et al*., 2006). There are a number of explanations for online solicitations of young children in particular. Adults, with an interest in young children can, for example, come into contact with children without an actual meeting in a physical environment. Social networking sites provide a range of facilities for gathering information (Kim-Kwang, 2009). Public directories on social networking sites contain a wealth of information, which are set out under various headings – groups,

age, name, email, location and gender. Profile information, comment and dialog tools and syndication feeds Really Simple Syndication, for example, provide offenders with mechanisms for monitoring their victims and gathering any new information uploaded by them. The task of identifying targets and gathering information about potential victims begins with perpetrators accessing directories on social networking sites and participating in chat rooms frequented by children (Kontostathis *et al.*, 2010). For example, depending on the privacy settings of the child and those on the child's network of friends, the acceptance of the offender as a friend on the social networking site will give the individual immediate access to the child's posts and profile pages. Most online sexual solicitations with children take place after an offender has gathered all the information about potential victims and assessed their amenability to being approached. The Provincial Court of Nova Scotia, in the trial of *R v Randall* (2006), was told that the accused logged into Internet chat rooms and scanned the profiles and communications before identifying his potential child victims. In *R v Gajjar* (2008), the offender used chat rooms on the Internet entitled "Family Sex" to engage in grooming activity. Online forums like these involve participants being favourably disposed towards sexually graphic communications. The offender in *Tector v R* (2008) used a pseudonym to send emails and text messages to persuade the victim to engage in sexual activity and even provided financial inducements. In *R v Dragos* (2010), the offender met the complainant on an Internet chat room called Habbo Hotel. This communication platform is designed to enable its users to discuss the sale of items of furniture for hotel rooms, and socialise with each other. The accused and the complainant used webcams to engage in non-contact sexual activity and communicated frequently through MSN. In all these instances, offenders tended to exploit the fact that electronic communications do not require face-to-face contact, and their belief that children were unlikely to disclose these interactions to parents or educators (Livingstone *et al.*, 2011). Webcams have also been used by individuals to record live images of children, which were subsequently stored, distributed or uploaded onto a website. In some cases, offenders have used images or conversations involving children they have been conversing with to coerce them into engaging in non-contact sexual activity, or arrange a face-to-face meeting. Malware have been used to allow individuals gain unauthorised access to a child's computer system, buddy lists, and webcams. On July 2010, a hacker broke into a child's computer, and gained remote access to the webcams of 150 girls (Deutsche Welle, 2008). Recently, a 25-year-old man coerced a 11-year-old girl to engage in acts of indecency in front of her webcam (Chong, 2010). He recorded these acts and threatened to release the images on the Internet unless she complied with his requests. According to the CEOP,

> there is also a marked trend of the use of webcam streaming chat sites, enabling offenders to interact either through instant messages and/or

> webcam to share previously captured footage or live-time images of abuse of children in their care. (Selgren, 2010)

It is not always the case that adults seduce young adolescents (*R v Grout (Phillip)* (2011)). Some children lie about their ages or even pretend to be older than they actually are, so that they can engage in non-contact sexual activity with persons they meet online. Many children, it seems, are at ease with interacting with strangers online (Wolak *et al.*, 2008: 342–3). Wolak, Finkelhor and Mitchell point to the findings from a survey which show that young children also use the freedom and anonymity offered by Web 2.0 technologies to gain the necessary sexual experience and confidence, which can later be used by them to develop relationships in the offline environment (Wolak *et al.*, 2006). In a study by Finkelhor, Mitchell and Wolak, if was found that 7 per cent of the children interviewed engaged in sexual conversations with strangers in chat rooms (Finkelhor *et al.*, 2000). Some children have been known to engage in the practice of setting up 'jailbait webcams' where teenagers create profiles on websites, with links offering sex shows and photographs for financial reward. The accounts also suggest why children's online activities generate so much anxiety and concern notwithstanding the fact that for the majority of children who do not like unsolicited sexual attention simple measures can be adopted to deal with such situations (Wolak *et al.*, 2006). The task of making accurate risk assessments is also complicated by the fact that children's online interactions with strangers cannot be invariably depicted as harmful. In an important study funded by the European Commission, it was found that 30 per cent of their sample of Internet users formed a friendship with someone they had met online (Livingstone *et al.*, 2005a). Eight per cent of them had met the person face-to-face. The majority of these meetings were positive, and where face-to-face meetings did take place, the child concerned often took a friend or parent with them, or told someone where they were going in advance. In a report issued by the Internet Safety Technical Task Force (ISTTF), it was noted that non-technology-mediated sex crimes against children outweighed those perpetrated through the Internet (ISTTF, 2008: 10). These accounts of the risk-prone nature of children's online activities illustrate the difficulties faced by parents and educators in making a proper assessment about how best to manage threats posed by online sexual solicitation as the traditional visual and safety cues are not present in electronic interactions.

Illegal or inappropriate content

Children and young people now have increased opportunities to access illegal or inappropriate content (Ybarra, *et al.*, 2005; Table 2.6). Communication platforms provided by Smartphones, video game and PlayStation consoles (e.g. Nintendo Wii or Sony PlayStation) can now be used by children to access a wide range of content without parental oversight (European Commission,

Table 2.6 Children's exposure to online pornography

Per cent	Exposure
57	Had contact with online pornography
38	Viewed pornography unintentionally
54	Not bothered by pornography
16	Do not like encountering pornography
9	Sent porn by someone they knew
10	Deliberately searched for pornography

Source: Livingstone and Bovill, 2005.

2011a: 52, 57). We can categorise problematic content that children can access or be exposed to into those that are illegal (e.g. child abuse content) and those which are inappropriate or harmful (e.g. pro-anorexia, bulimia and dating websites). In many countries there are content classification schemes which define the subject matter that can be made available to a general audience and those which are illegal. Children's access to and use of the Internet can lead to potentially harmful or age-inappropriate content being accessed either deliberately or inadvertently. A number of websites hosting adult content do not provide effective age-verification controls – most websites providing such content only provide a notice requiring the visitor to verify that they are of an age where access to adult content is permissible. Search engine operators like Google or Yahoo provide tools which enable individuals to access adult material, images and videos. A number of websites also host user-generated content, which can be accessed for free, and do not have effective age-verification tools. The lack of effective age-verification controls is confirmed by surveys and reports (Livingstone *et al*., 2005a; Ybarra *et al*., 2005).

OfCom found that around 16 per cent of children aged 8 to 15 encountered inappropriate or violent content when using Web 2.0 technologies (2006: 45). A survey of children aged 9 to 10 and 12 to 14 across 29 countries found that children had either encountered violent or pornographic websites or harmful content (Hargrave, 2009: 8). This is a finding that is also mirrored in national reviews undertaken in countries like the United States and Australia (OSTWG, 2010: 14–16; ACMA, 2009b: 43). The studies did, however, indicate that children regarded encounters with problematic content as being of less concern than, for example, harms caused by malware and viruses. The 2008 Eurobarometer Survey revealed that over 65 per cent of parents feared that their children may be exposed to sexual or violent content or images of an explicit nature (Eurobarometer, 2008: 5). Children's exposure to inappropriate and harmful content is an important

online child safety issue. Many children reportedly use the Internet to access inappropriate and harmful content like self-harm and suicide (Royal College of Psychiatrists, 2010: 52). What concerns educators and parents is that whilst a number of websites provide children with invaluable assistance, there is some evidence of certain websites normalising the practice of self-harm and suicide (Whitlock *et al*., 2006; Hargrave *et al*., 2006). More worryingly, it has been reported that children are increasingly accessing information from online pro-eating disorder and self-harm communities (Fox *et al*., 2005: 944–71). Self-harming behaviour, for example, is now regarded as a major public health problem (Hawton *et al*., 2005: 891–4). The Royal College of Psychiatrists also reported that 4 in 1,000 people in the United Kingdom have harmed themselves (Royal College of Psychiatrists, 2010). Children as young as eight years old have been found to harm themselves and adolescent girls were more likely than boys to engage in the practice (Royal College of Psychiatrists, 2010: 31). One in five schoolchildren with a history of self-harming first discovered about self-harm from material they accessed online (Whitlock *et al*., 2006). It also appears that without timely intervention those children who are most at risk or vulnerable are likely to accept the accuracy and reliability of the information presented to the detriment. There is also particular concern with regard to children's access to racist or xenophobic material on websites, since it is felt that consumption of such content could encourage prejudice, reinforce stereotypes and even incite bullying or other forms of peer victimisation (Ray *et al*., 2001). In addition to these concerns other technological affordances like emails, IM and social networking sites now provide individuals with another medium for engaging in race- or gender-related abuse (Defeis, 1992; Blumenfeld *et al*., 2010). The Byron Report advocated the use of education and regulatory mechanisms (e.g. codes of practice) to reduce the availability of harmful and offensive content (Byron, 2004: paragraph 4.34–43). Interestingly, the Report did not regard the requirement that web hosts remove material about harmful behaviours from their sites as a sustainable risk management response (ibid.: paragraph 4.33). One recurring view is that the public interest would not be served by blocking access to such content since "[b]anning such content risks driving vulnerable young people away to more obscure sites" (Byron, 2008: paragraphs 4.35–36) Even if the UK government did decide to make access to inappropriate content unavailable to children, these are likely to provoke objections from industry on the ground that the putative harms are more effectively addressed by educators and parents through the provision of relevant safety information and tools. In addition to this, it should be noted that technical solutions like filtering and blocking have undoubted limitations as a content regulatory mechanism. In a recent study funded under the SIP it was reported that many Internet filters did not adequately regulate the various forms of age-inappropriate or harmful content found on social networking sites, chat rooms and blogs (European Commission, 2011a).

Peer victimisation

There is general consensus that communication technologies now bring to the forefront increased opportunities that mobile phones and the Internet provide for victimisation (Lenhart, 2007). Bullying can, for example, take place through texts, emails, mobile phones or on social networking sites. Acts of coercion include the unauthorised distribution of texts and embarrassing images of children and film clips of victims being subjected to assaults, known as "happy slapping". Private information posted online have also been copied and distributed without the owner's consent, with the aim of causing distress. In a recent study undertaken in Iowa, United States, it was found that transgender bullying was quite common amongst young adolescents (Blumenfeld *et al.*, 2010). Blumenfeld and Cooper noted that lesbian, gay, bisexual and transgender individuals were increasingly subjected to victimisation by peers on social networking sites and other communication platforms (2010: 2–10). We should also add to this category of victims children who are disabled or who have particular learning difficulties (*TK v New York City Department of Education* (2011)). A three-year study in Australia noted an increase in peer victimisation (Cross, 2009). This study was commissioned by the Australian government amidst growing anxieties over the use of communication technologies to engage in "covert bullying" and the findings confirm growing concerns shared by policymakers in many countries about the scale of peer victimisation and its impact on victims and perpetrators (see Table 2.7).

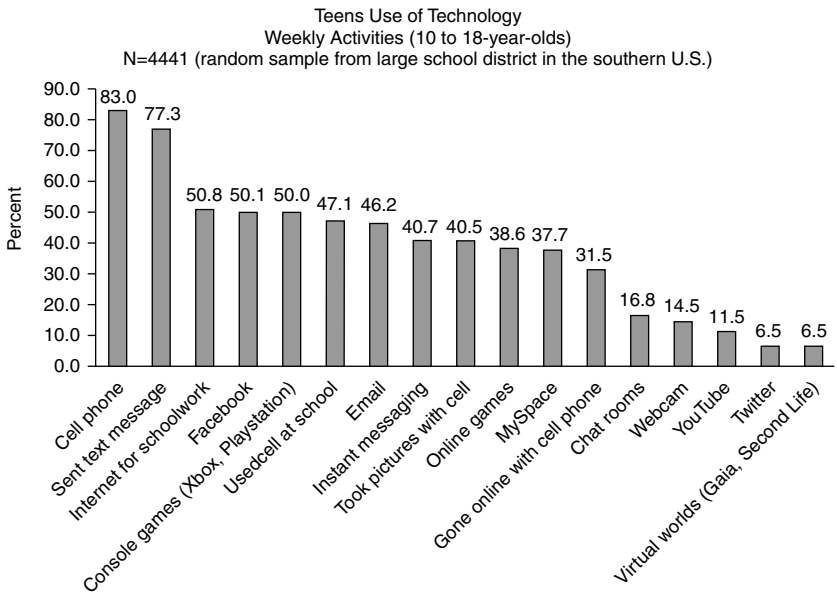
In their studies on children's use of technologies Hinduja and Patchin suggest a close correspondence between increased consumption of Web 2.0 technologies and the rise in children's exposure to victimisation and, in a number of cases, participation in the deviant activity (see Tables 2.8 and 2.9).

These communication platforms are also venues where peer victimisation is encountered (Kowalski *et al.*, 2007; Patchin *et al.*, 2010a,b). Consequently,

Table 2.7 Web 2.0 technologies and peer victimisation

Email/IM	**Social networks**	**Mobile phone**	**Virtual worlds**
Forwarding secrets and private communication	Image defacing	Happy slapping	Targeting peers on the grounds of gender, race or religion
	Creating false profiles	Photographs	
	Forwarding private images/text		
	Listing "unpopular" peers		

Table 2.8 Children's risk-prone activities



the misuse of technologies and departure from social or ethical norms to humiliate and cause maximum upset illustrates how such activities can escalate into child protection issues.

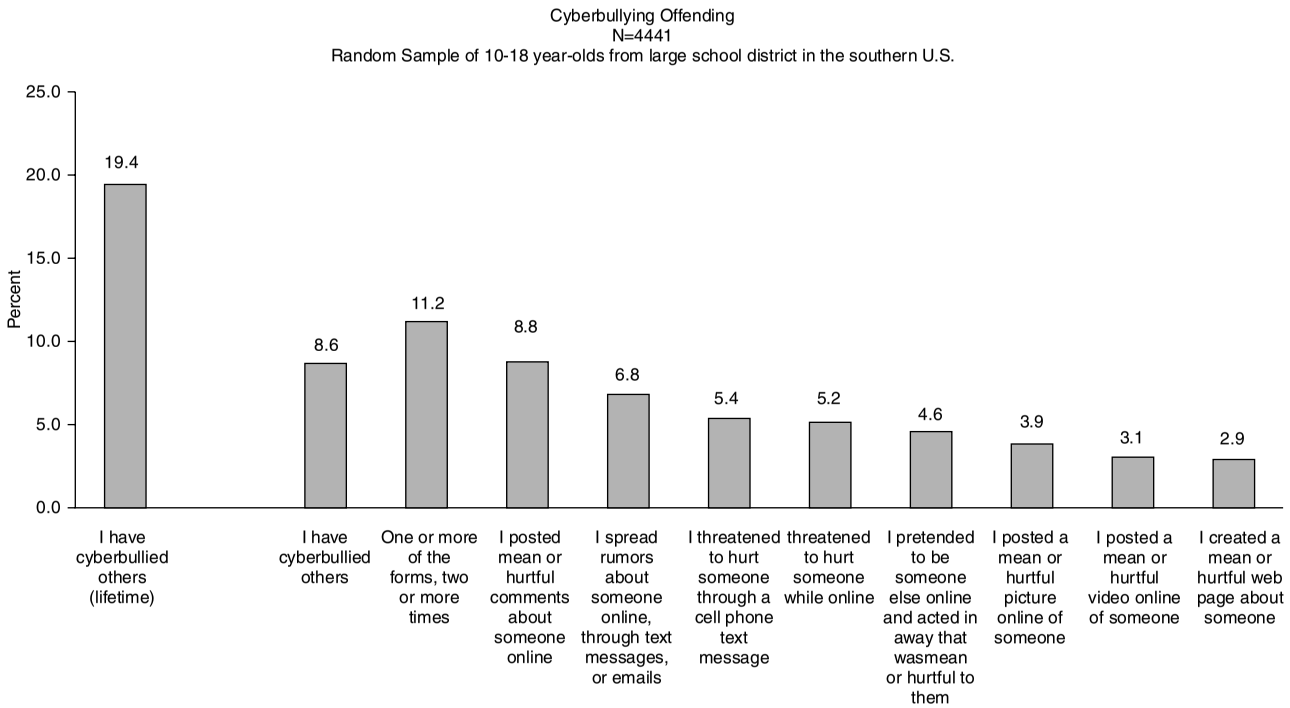
Framing the risk facing children is in itself a complex endeavour. For example, in *TK* (2010), the peer victimisation activities included the making of prank phone calls to the victim and drawings depicting the victim in a negative light. At the recent White House Conference on Bullying Prevention, over 40 per cent of the educators and support staff surveyed reported that bullying was a major problem in their schools (White House, 2011). Cyberbullying has been described as a type of conduct where

> someone repeatedly uses the Internet or a mobile phone to deliberately upset or embarrass somebody else. It is intended to harm others and can include sending mean or nasty words or pictures to someone over the Internet or by mobile phone. (ACMA, 2009c: 63)

Another view is that cyberbullying involves a

> repeated or sustained pattern of intentional cyber-attacks that causes distress and is directed against a specific student or group ... [it can] also be a multi-faceted or multi-step campaign of humiliation or hostility that causes distress and is directed against a specific student or group. (AMF, 2009: 4)

Table 2.9 Web 2.0 Technologies and online child safety incidents



The absence of a settled meaning or understanding of the term makes it difficult to frame the problem, and more often than not can lead to safety measures and strategies that adopt a managerial approach to risk management – "delete offensive texts and emails", "do not upload information on websites" and "mobile phones should not be used during school hours". The rise in bullying, particularly through the use of Web 2.0 technologies, cannot be simply attributed to the existence of a legal and policy vacuum (Shariff, 2009) or to the fact that new technologies enable children to express their aggression (Hinduja *et al.*, 2009). In their study, Ybarra and Mitchell highlight the close relationship between online and offline bullying (Ybarra *et al.*, 2004). In some instances, it was found that those who were victims in the offline environment used the online environment to redress the power and social balance when inflicting distress on their perpetrators (Patchin *et al.*, 2006; Ybarra *et al.*, 2007). In one survey, 56 per cent of the online aggressors claimed to have been the subject of offline victimisation (Ybarra *et al.*, 2004). Interviews commissioned by ACMA reported that a child's exposure to peer victimisation incidents also showed a marked increase with the age of the child (ACMA, 2009c: 66).

Technology-mediated victimisation has three features that incentivise "an overt, intentional act of aggression towards another person online" (Ybarra *et al.*, 2004: 1038) or "wilful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices" (Hinduja *et al.*, 2009: 5). These are the anonymity that the bully leverages to victimise an individual; the viral nature of the victimisation (i.e. many to one) and the lack of visibility in the consequences of the victimisation. Swearer highlights a number of risk factors that contribute to bullying and victimisation: individual risk factors (e.g. age, gender, socio-economic status, ethnicity and religion), peer-group risk factors (e.g. homophily and deviancy), school risk factors (e.g. educators' attitudes, school architecture, belonging, academic and social engagement) and family risk factors (e.g. violence in family, family upheavals) (Swearer *et al.*, 2010).

The media spotlight on peer victimisation has elevated bullying into public and political consciousness. Such is the gravity with which peer victimisation is viewed that the White House was moved to convene a Conference on Bullying Prevention. Interestingly, the First Lady remark's illustrates the close interplay between heightened public anxiety, parents' individualisation of fears for their children's well-being and the media's definition of the problem:

> I want to thank all of you for joining us here today to discuss an issue of great concern to me and to Barack, not just as President and as First Lady, but as a mom and a dad. And that is the problem of bullying in our schools and in our communities...

> As parents, this issue really hits home for us. As parents, it breaks our hearts to think that any child feels afraid every day in the classroom, or on the playground, or even online. It breaks our hearts to think about any parent losing a child to bullying, or just wondering whether their kids will be safe when they leave for school in the morning.
>
> And as parents, Barack and I also know that sometimes, maybe even a lot of the time, it's really hard for parents to know what's going on in our kids' lives…
>
> But parents aren't the only ones who have a responsibility. We all need to play a role – as teachers, coaches, as faith leaders, elected officials, and anyone who's involved in our children's lives. And that doesn't just mean working to change our kids' behavior and recognize and reward kids who are already doing the right thing. It means thinking about our own behavior as adults as well. (White House, 2011).

Many of the observations made by Beck resonate in this excerpted speech – heightened anxiety, risks generated by information flows, children viewed as being vulnerable to risks as well as being perpetrators of online safety incidents and the need for risk management strategies. This is not to say that efforts to combat peer victimisation are not being made (Olweus, 2007; Sampson, 2002; Mencap, 2007). The public health model, which regards targeted interventions and support, creating appropriate school culture of respect and civility, social skills training, monitoring and engagement with parents and the community as a governance strategy, is an important step towards creating a "whole-school/community" approach to bullying prevention (Chamberlain *et al.*, 2010).

Managing insecurity (anxiety) and reflexive modernisation

Risk is conspicuous even though Web 2.0 technologies and network publics appear on the surface to involve nothing more than participatory genres and cultures of self-presentation and identity experimentation. Questions about how we manage risks the way we do, the evidence informing the conclusions drawn from the relationship between technology and risks, the assumptions we make about children's use of media and the evolving role of parenting cultures are very much a part of living in the risk society (Beck, 1999). Buckingham is right when he alludes to children being regarded as natural subjects for regulatory oversight, since "assumptions about who these other people are – and, in this case, about what 'childhood' is, or should be" (2000: 104). The threat of technology-enabled crime has given rise to a growing demand for strategies for prevention and control, particularly in the area of online child exploitation. Mazzarella regards societal safety concerns borne out of interest in children's immersion in communication technologies as indicative of cultural attitudes towards children – a body of individuals requiring constant supervision and monitoring (2007: 46–7).

Two further observations need to be made with regard to the process of reflexive governance in the area of online child safety. First, risk-taking behaviour amongst children is conceptualised in negative terms whether it is in virtual worlds, social networking sites or network publics. It is readily assumed, for example, that children's exposure to potential (or perceived) contact and non-contact risks results from their willingness to disclose personal identifiable information online, their immaturity and lack of understanding about the nature of the risks. It is true that one of the consequences of being connected with communication networks is that everyone is potentially at risk, even though paradoxically, it is unlikely to be experienced by all individuals. Interestingly, children's online activities and use of Web 2.0 technologies are singled out and described as "risk-prone behaviours" (ITU, 2010b: 16). It is important to acknowledge that many children who are solicited online by adults do not arrange to meet them. Social networking sites, chat and IM platforms have tools to block and report unwanted contact. Recently, Facebook created a social abuse reporting mechanism for individuals to alert their "friends" about potential abusive or inappropriate activity. Ironically, rather than demonise activities and behaviours as "risk-prone", it should also be remembered that it is through the norms of sharing and engagement that a community of networked sociability can be leveraged to reinforce civility and respect. The integration of civic responsibility and appropriate behaviour norms through design solutions in effect allocates to children some of the responsibility for policing the networked community. In viewing all online activities as "risk-prone" or "risky" it has been suggested that we may attach little importance to the value of positive risk taking in promoting good decision-making skills, developing resilience and enhancing children's ability to respond to online incidents in a safe and responsible manner. One is also inclined to agree with Gill, when he suggests that curbing a child's ability to take reasonable risks may be counterproductive and have the unintended effect of leading them to engage in more dangerous and unsupervised activity (Gill, 2007: 15–16). Second, the culture of reflexive governance has also led to the institutionalisation of risk management. The State has an obvious role in allaying public fears and concerns, as suggested by the former Home Secretary David Blunkett:

> Public protection, particularly of children and the most vulnerable, is this Government's priority ... But sexual crime, particularly against children, can tear apart the very fabric of our society. It destroys lives and communities and challenges our most basic values. (Home Office, 2002: 5)

In a House of Commons Select Committee hearing, the following observation was made about the technology and its implications for parents:

> However, anyone who regularly watches television or reads the press is likely to have become aware of growing public concern in recent months

> at the Internet's dark side: the easy availability of hardcore pornography, which people may find offensive, the uploading by ordinary people of film of real fights, bullying or alleged rape, or the setting up of websites encouraging others to follow extreme diets, or self-harm, or even commit suicide. In particular, there is *increasing anxiety among parents about the use of social networking sites and chatrooms for grooming and sexual predation*. (House of Commons, 2008: 7) (my emphasis)

As a broad statement of intent, these observations appear to overstate both the context and experiences of many children and consequently advocate the need for greater protection and oversight of children's online activities. Management of theoretical risks rather than those encountered by children becomes the focal point of the precautionary approach to child safety governance. Crucially, the difficulties in assessing the scale of the risks, the use of risk-based regulation to require shifts in behaviour of all stakeholders (including children) and the trade-offs involved also illustrate the challenges and potential objections that may be encountered under the MSIG model of institutional design and governance (Hood *et al*., 2001: 181–4).

Children's risk-prone activities, individualisation of risks and moral panics

Safeguarding children in the online environment can be viewed as mobilising cultural attitudes towards children and risks – the individualisation of risks leads to risk management techniques focusing on perceived and actual threats (Giddens, 1991: 198). Policymaking forums at national, regional and supranational levels now adopt risk-based regulatory strategies, which engage industry, experts and other stakeholders in identifying and assessing the risks faced by children. Holmes has questioned the imbalance in online child safety debates (Holmes, 2007). The Byron Report is singled out for magnifying the risks faced by children in the online environment rather than emphasising good online behaviour and appropriate computer use practices (Holmes, 2009: 1175). Risk discourse manifests itself in a number of ways in child protection policymaking. McAlinden, for example, highlights how media construction of sex offenders contributed to legislative responses to regulating sex offenders (2007: 11). Gerbner articulated similar discourses about children's safety and well-being being compromised by their exposure to television (Gerbner *et al*., 1976). It has been suggested that anxieties surrounding children are also magnified by the disproportionate emphasis placed by both the media and policymakers on the threat landscape. A "moral panic", according to Stanley Cohen, is when a

> condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests; its nature is presented in a stylized and stereotypical fashion by the mass media; the moral barricades are manned by editors, bishops, politicians and other right-thinking people. (1972: 1)

The concerns raised by the Attorney General's press release (noted at the start of Chapter 1) could be regarded as addressing a "condition", "episode" and a "group of persons" which pose threats to children's safety and well-being. Online service providers, parents and educators, according to the definition of a "moral panic", would seem now to be the digital equivalent of "bishops" and "right-thinking" individuals. The media reporting could also be seen as one example of risks facing children being presented in a "stylized and stereotypical fashion" (Ungar, 2001; Garland, 2008). The law enforcement response in relation to the presence of online sexual predators and potential threats for children is depicted as legitimating the elevation of safeguarding children as a social and moral obligation on all adults and businesses in society. The risk-based regulation model extends to corporate stakeholders – social networking sites and mobile phone providers now become the focal points for allocating blame and responsibility (Critcher, 2008). The mischaracterisation of the precautionary principle will only serve to deflect "from the truth and thus simply makes it more difficult to figure out what we should do to effectively address the situation" (Ohler, 2010: 144). The European Commission was clear in its Communication that

> [t]he precautionary principle, which is essentially used by decision-makers in the management of risk, should not be confused with the element of caution that scientists apply in their assessment of scientific data. (European Commission, 2010: 3)

Determining what is a proportionate policy response continues to prove to be an ongoing challenge since the construction of risks and their alignment with child abuse and victimisation evoke strong emotive reactions (Ostertag, 2010). Increased regulatory interventions tend to fuel rather than allay concerns. This is hardly surprising since

> the government in many ways reinforces adult perceptions of risk to children by reacting to public and media pressure rather than responding to evidence. This can mean that policies that reflect and reproduce risk anxiety rather than reflecting a proper, informed evaluation or appraisal of the real dangers facing children. (Madge *et al.*, 2007: 22)

Public anxiety and concerns leading to moral panics pose considerable problems for policymakers (Goode, *et al.*, 1994). McAlinden regards the cycle of moral panic as reconstructing social reality, resulting in perceived risks being transformed into a discourse about a society "full of sexual predators" (2007: 11). The process of "constructing a social problem" has a more immediate relevance – it leads to a cycle of, what Beck regards as, heightened anxiety and public expectation that policymakers respond to the critical tensions raised by children's exposure to Web 2.0 technologies (Hawkins *et al.*,

1983). Taking the MySpace incident, which opened the discussion in the book as an example, very little weight or importance was attached by the Attorney General to the practical question of whether the online services provider had taken appropriate and reasonable measures in enhancing the safety of its products and services. Without MySpace's due diligence protocols, 90,000 registered sex offenders would not have been identified in the first place. The Sentinel SAFE software, which is funded and developed by MySpace, cross-references the information of its 130 million users with the national database of known registered sex offenders. By focusing on the uncertainty generated by the presence of the registered sex offenders, risk management becomes inseparable from managing uncertainty – consequently, it seems that in the absence of absolute proof that uncertain risks are eradicated, social networking sites are to be viewed as unsafe for children (Ungar, 2001: 273). The press release also contributes to increased preoccupation with managing uncertainty, as it appears to imply the existence of an ideal or appropriate risk management response. A recent illustration of the uncertain boundaries between moral panics and legitimate risk management governance can be seen in the claim made by CEOP to have made the online environment safer, following the adoption by social networking sites and a number of online service providers and ISPs of the ClickCEOP reporting button (CEOP, 2009: 15). Without overstating the obvious, if this claim holds true, it is difficult to see why the same could not be said for the efforts made by MySpace or Facebook in adopting the proactive measures that they have. Accordingly, as risk is pervasive in society, and is accentuated by networks and information flows

> fear of crime is a particularly apt discourse within the modernist quest for order since the risks it signifies, unlike other late modern risks, are *knowable, decisionable, (actionable)*, and potentially *controllable*. In an age of uncertainty, discourses that appear to promise a resolution to ambivalence by producing identifiable victims and blameable villains are likely to figure prominently in the State's ceaseless attempts to impose social order. (Holloway *et al*., 1997: 265)

As Fortin points out, policymakers struggle to find an appropriate balance when designing systems to manage complex and intractable issues (Fortin, 2010: 586–7, 590–1). By way of conclusion to this chapter, it may be useful to assess how the crossover between moral panics, risks and governance takes shape in evolving parental cultures.

Evolving parental cultures in a risk-averse society

For many parents and educators, the Internet and mobile technology are seen as increasing children's vulnerability and exposure to inappropriate content, sexual exploitation and peer victimisation (OfCom, 2006; Table

2.10). The findings from the Eurobarometer Survey, noted below, can be used to illustrate Beck's central ideas about living in the risk society, in particular for evolving parental cultures (Eurobarometer, 2008).

Risk anxiety is particularly noticeable in relation to online sexual solicitation (60 per cent) and exposure to sexual and violent content (65 per cent), but does not appear to be particularly high in relation to peer victimisation (54 per cent) or exposure to age-inappropriate or harmful content (55 per cent). Parents anxieties about children being sexually victimised or exposed to sexually explicit content is not new – it should also be noted that it is not entirely clear whether the Internet accentuates these anxieties. Another interesting finding relates to the number of parents who indicated that they were not really worried about online sexual solicitation (36 per cent), exposure to sexual and violent content (31 per cent) or exposure to age-inappropriate or harmful content (41 per cent). It seems that parental anxieties were much higher in cases where they did not use the Internet themselves, in contrast to those who did use the Internet (2008: 30). Additionally, where low scores were highlighted, it is unclear from the survey whether

Table 2.10 Parents' perspectives of online child safety incidents

Risks	Very much worried	Rather Worried	Rather not Worried	Rather not worried at all	Do not know/not applicable
Might see sexually/ violently explicit images on the Internet	45	20	14	17	4
Victim of online grooming	46	14	13	23	5
Access to self-harm, suicide, anorexia content	39	16	15	26	5
Bullying	37	17	18	23	5
Might see sexually/ violently explicit images via the mobile phone	37	14	13	26	11
Mobile phone bullying	34	15	14	25	11
Might give out personal/private information online	26	21	24	25	4

Source: Flash Eurobarometer, 2008.

Table 2.11 Parents' strategies regarding children's use of the Internet

Parental mediation	Dialogue about online use (per cent)	Remain in vicinity when computer used (per cent)	Co-surfing (per cent)	Check the computer later to see which sites child visited (per cent)	Check whether your child has a profile on a social networking site (per cent)	Check the messages in your child's email account/ IM service (per cent)
Parents' Internet use						
Non-users	60	44	28	24	17	18
Occasional users	75	65	40	44	29	26
Frequent users	76	60	36	44	31	24

Source: Flash Barometer, 2008: 39.

parents were in effect underestimating the realities of children's experiences (Livingstone *et al*., 2011; Table 2.11).

Whilst parents adopt different safety enhancing strategies, the findings show that greater control tends to be exercised over the child's Internet use – these findings can be interpretated in one of two ways. First, parents with greater ICT competence and knowledge of the safety issues appear to engage more fully with a child's online activities. Second, the lack of supervision could be attributable to a number of factors (e.g. level of ICT competence, limited awareness of the risks or trust in children's online activities). The findings from the Flash Barometer Survey also correspond with a similar study undertaken by ACMA in 2010:

> Parents of 8 to 11 year olds reported that they became increasingly concerned about cybersafety issues because their children were now at an age where being online was an integral part of their school education and their social life. (ACMA, 2010b: 7)

Another way of interpreting the Flash Eurobarometer findings is to view the survey results as illustrations of the way the logic of information flows contributes to the convergence of risk anxiety, constructions of childhood and parenting cultures. Youn has noted a number of mediatory strategies adopted by parents when socialising their children to the risks surrounding Internet activity (2008: 362–88). Parents, for example, view their role in establishing rules on Internet use at home as an integral aspect of their social and moral responsibilities towards children. Those who have a better understanding of the scale and extent of the risks may tend to supervise and monitor children actively. Parents with younger children may be more protective and consequently co-surf or check on their child's online activities (Mesch, 2009). McCarty remarks that as parents acquire information of their child's perceived online risky behaviours, it may also lead to more active parental oversight (McCarty *et al*., 2011: 169–74).

The characterisation of children's lives as being more risky than those of adults has also resulted in a discernible shift in the way parents view the responses expected from them. This is a view expressed by Knaak, who has argued that the ideology of risk has contributed to evolving social norms that surround the role of parents in managing risks encountered by children at home, school and elsewhere (Knaak, 2009). It is, for example, noticeable that many parents justify purchasing mobile phones for their children on the grounds of ensuring the child's safety and allaying parental anxieties (Haddon, 2002: 118). The move away from the "bedroom" culture (e.g. children using computers in the privacy of their bedrooms) is also indicative of the evolving parental views that children's exposure to risks can only be minimised in spaces where they can be monitored (Haddon, 2002). Knaak makes an interesting observation, namely, that responsible parenting is now

viewed very much through the lens of institutional and regulatory processes for managing risks (Knaak, 2009). There is also a noticeable trend in the way anxieties about managing risks also lead to greater intervention by industry and government in creating a safer environment for children (ITU, 2008a, 2009d,e). Strategies to promote trust and confidence continue to be merged with discourses on empowerment and responsible parenting. Parents are not regarded as passive actors, as risk management become institutionalised; there is an expectation that they be seen to take an active part in the daily online and offline lives of their children. These developments can at a very abstract or theorised level be seen as impressing on adults in society that a child's well-being and safety is best assured within an institutional framework of defined rules on monitoring computer use and instilling risk-averse behaviour (Hier, 2003). Networks and information flows have led to a gradual weakening in parental authority and control over children (Lamborn *et al*., 1993). In some cases, as Web 2.0 technologies accelerate the "de-traditionalisation" of the social paradigm, parents now seek to bolster their trust by turning to their own experiences, media accounts of threat levels and assessments made by experts and institutions (Hier, 2003). For example, ACMA, like many regional and national institutions, continues to assist parents in discharging their ethical and social obligations by raising their awareness of online safety issues (ACMA, 2010b: 1). This view of the role of institutions in shaping parenting cultures can be regarded as another example of living a risk society where

> the parent is construed as unable to risk-manage effectively without professional "support". Cultural norms ... thus construct the "good/responsible mother" as the mother who is alert to the manifold risks posed to her child(ren) by contemporary society, and considers it her job to manage these risks through reference to expert opinion. (Lee, 2008: 469)

It is also an illustration of how the patriarchal framework within society continues to negotiate the disruptive tendencies of Web 2.0 technologies.

Conclusions

One reason that "online child safety" continues to dominate policymaking is that it has rhetorical purchase for a number of child welfare and political entities. The claims that reporting mechanisms have saved a number of children does not address some of the crucial normative issues at stake when risks are "institutionalised" and filtering and blocking are seen as value free. It is therefore not surprising that appeals to policymakers, parents, educators and law enforcement that the fears and anxiety should be kept in perspective continue to go unheeded. The main focus has been directed at the interplay between design, convergence and risks and its significance for the

policy choices governments, regulators, and industry have to grapple with. This is a considerable challenge made all the more complicated by the fact that our preoccupation with online sexual predatory activity, exposure to illegal or harmful content and peer victimisation cannot be easily disentangled from societal constructions of childhood and discourse on risks and safety. The chapter has provided some examples and reasons why this might be the case. Whilst it is true that childhood is politicised and constructions of the "victim" child continue to define much of how we think about societal obligations to children, this chapter has identified an equally important dimension – how increased risk consciousness can be influential in shaping institutional and parental responses towards children's safety and well-being. It is important to recognise how such constructions of risks can shape the way safety responses like monitoring, surveillance and restrictions on children's access to and use of Web 2.0 technologies become operative norms in the networked society. Beck's insights and of those who have examined the impact of "risk consciousness" on parenting cultures reveal some of the governance implications arising from the discourse on risk and its significance for childhood in the networked society. We need to keep these considerations in mind since the architecture and the design principles that led to the exponential growth of the Internet continue to provide the critical infrastructure for economic and social activity (OECD, 2010a: 38; Schewick, 2010: 387). As policymakers aim to respond to the governance challenges, we need to be equally mindful that these developments, even in the domain of the criminal law, are

> set against the backdrop of a heightened sense of risk consciousness, "the new etiquette" of caution, fear and danger has distanced itself from judgments about what is morally proper or acceptable, becoming transposed into discourses of safety, security and communal living ... To put this succinctly, as anxieties endemic to the risk society converge with anxieties contained at the level of community, we should expect a proliferation of moral panics as an ordering practice in late modernity. (Hier, 2003: 19)