Sonia Livingstone

e-Youth: (future) policy implications: reflections on online risk, harm and vulnerability

Conference Item: Keynote Address

'e-Youth: (Future) Policy Implications:

Reflections on online risk, harm and vulnerability'

Sonia Livingstone, LSE

Keynote presentation to the conference,

e-Youth: balancing between opportunities and risks,

University of Antwerp, May 2010.

Introduction

Most children in the world's wealthy countries use the internet at home, school and elsewhere, with ever more children gaining the broadband and mobile access that thoroughly embeds online activities into the timetables and spaces of their daily routines. Accompanying this notable change in the conditions of childhood, education and participation, a growing body of academic, public policy and market research is charting the unfolding nature and scope of children's use of the internet, revealing the considerable opportunities it affords, the intriguing and complex digital literacies that children are gaining and the diverse pleasures of use.

At the same time, there is growing concern that online opportunities are accompanied by a diverse array of risks. Before any policy actions can be formulated, a clear view of the evidence base is vital. The EU Kids Online network classified online risks to children in terms of *content risks* (which position the child as recipient, generally of mass produced content though increasingly also of user-generated content), *contact risks* (in which someone contacts the child, requiring him or her to participate in some way, if unwittingly or unwillingly) and *conduct risks* (where the child is an actor, generally as part of a peer to peer or networked interaction), as shown in Figure 1 (Hasebrink, Livingstone, Haddon, & Olafsson, 2009).

	Content Child as receiver	Contact Child as participant	Conduct Child as actor
Aggressive	Violent/ gory content	Being bullied	Bullying
Sexual	Pornography	Grooming	Sexual harassment
Values	Racist/hate	Ideological persuasion	Self-harm
Commercial	Embedded marketing	Privacy /data abuse	Downloading Gambling

Figure 1: Classification of online risks (with exemplars)

Summarising some 400 studies across Europe, the EU Kids Online network further estimated that five in ten teenagers have given away personal information to others online, four in ten have seen online pornography, three in ten have seen online hate or violent content, two in ten have received bullying or nasty messages and one in ten has gone to a meeting with someone first met online. This suggests that content risks are the most common, followed by contact risks; less is known on a cross-national basis about conduct risks, where the child is positioned as perpetrator rather than victim or, indeed, about many other risks on the policy agenda. Although evidence of risks is difficult to obtain and open to methodological challenge, researchers do seem to be reaching some consensus on how to ask children about these risks, strengthening the evidence base and thus surely aiding policy makers in determining appropriate action.

But this evidence base faces some problems. One is that it becomes quickly out of date, given continual changes in:

- *The technological environment* - the array of increasingly personalised, networked, convergent and mobile media products and services available to children;
- *The social environment* - the changing contexts of media use, as digital and online media become increasingly integral to all spheres of life, blurring boundaries of home and school, public and private;
- *The regulatory regime,* whereby new forms of national and transnational governance, and new kinds of self- and co-regulatory institutions emerge, with varying accountability and effectiveness;
- *The conditions of childhood*, notably the practices of children who are increasingly though unevenly digitally literate, variously more creative and participatory than merely receptive, ever more reliant on peer compared with adult relations.

While challenging, and requiring a sustained research effort, this problem is largely *practical* – what is required is sufficient research funding, ingenuity in research design, and careful attention to the changing conditions of children's online experiences. This paper focuses on *four more difficult problems* – the nature of risk, harm, vulnerability and the difference that the internet makes.

Consider one survey result that recently became widely known: in December 2009, Pew 's Internet & American Life project reported that 15% of 12-17 year olds with a mobile phone had "received sexually suggestive nude or nearly nude images of someone they know" (Lenhart 2009; p.2). "Sexting" quickly became the latest risk, with policy makers, law enforcement and educators springing into action. But some pressing questions arise. First, does this matter, is it harmful? Then, if it is, which teenagers are involved, i.e. which are vulnerable? Third, is this problem new, worse than before, making new media somehow culpable? Not asking these questions can seem to imply that all children are 'at risk', that the worst experience known to occur to one child is waiting to happen to every child. To avoid the media-amplified moral panics that stimulate anxious calls to restrict children's internet access, increase surveillance or legislate against online freedoms, research must go beyond the risk headlines.

Let us begin somewhere other than the internet, for, although the internet is relatively new, with the emergence of new risks always threatening to outpace the ability of researchers, policy makers and the public to keep up with them, a long tradition of research exists about the nature of risk, harm and vulnerability 'offline', including a substantial body of work on risk in children's everyday lives (Bradbrook et al., 2008; Coleman & Hagell, 2007; Feinstein & Sabates, 2006; Finkelhor, 2008; Munro, 2008; Schoon, 2006). This literature is useful, first, in clarifying these central terms, for in relation to the internet, there is much confusion – is exposure to online pornography really risky? If yes, does that mean it harms all children? If some can laugh it off and ignore it, what does that tell us about those who are upset? Maybe the internet isn't really risky, it's just that some children are vulnerable? Or, does such a label stigmatise children? Second, this literature may be useful in raising empirical questions about the relation – variable, multifaceted and contingent though it is - from risk to harm, in both the immediate and long-term. What does this more established knowledge base regarding offline risk offer to the newer field of inquiry into online risk? Or is the online environment too different for such continuities to apply?

Reflections on risk

What is risk? Beck (1986/2005: 21), theorist of the 'risk society' argues that, "risk may be defined as a systematic way of dealing with the hazards and insecurities induced and introduced by modernization itself." Until the modern era, he argues, societies were preoccupied with natural *hazards* (e.g. flooding, volcanoes, drought, plagues). Since these are uncontrollable in themselves, people can only seek to manoeuvre around them. By contrast, today, societies are increasingly preoccupied with *risks* of our own making, being,

> … concerned no longer exclusively with making nature useful, or with releasing mankind from traditional constraints, but also and essentially with problems resulting from techno-economic development itself… 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. (p.19)

A risk, in short, stems from the conditions of modern life rather than from outside them. Unlike the problem of dealing with a volcano, where one can only *respond* to an inevitable if unpredictable hazard, dealing with the problem of online grooming or bullying invites us to *anticipate* risk when designing the online environment as well as to consider how such risks should be responded to afterwards. Following Giddens (1991), in today's reflexive modernity, we cannot be innocent of likely, if unintended, consequences of institutional actions, or of what prior research has shown. For example, now to design a social networking site for small children without anticipating possible abuses by ill-intentioned adults would be naïve.

Crucially, however, 'risks describe probabilities and not certainties' (Schoon 2006: 10), resulting in an array of approaches to calculating risk. Klinke and Renn (2001) distinguish:

- *risk assessment* (a scientific calculation based on risk probability and magnitude – i.e. likelihood x consequences),
- *risk evaluation* (a usually political judgement of the acceptability – to the public, to policy makers - of a given risk),
- *risk management* (the institutional/policy process of reducing risks to a level deemed tolerable by society).

This may clarify the at-times confused discourse of child online safety:

- Being exposed to pornography online is, we may say, a risk in the sense that it is associated with a certain likelihood and magnitude of harm – hence it is important that the evidence base measures these.
- The identification of online risk does not imply that harm will follow, nor that all users will be equally affected; rather, it is a probabilistic judgement regarding an outcome that depends on the particular and contingent interaction between user and environment.
- It may be dealt with by conducting a risk evaluation which, in turn, establishes the legitimacy of risk management (such as the development of regulatory institutions or user tools and tactics).
- And since, following Beck, online risk does not arise inevitably, this risk management can be reactive or proactive, and it can focus on the actions of the individual (the user) or the design of the socio-technical environment (the internet).

- Or, indeed, nothing may be done – the risk may not be judged unacceptable (it may be tolerated up to a point) and/or it may not be managed for wider political, economic or social reasons which are nothing to do with the risk assessment.

So far so good. But let us remember what it is we measure – that 15% of teenagers receive sexual messages, that 40% have seen online pornography, and so forth. These 'online risks' in 'cyberspace' are often compared with the popular 'offline risk' of a child crossing the road. Just as with the latter, where we calculate the risk and then seek to manage both the child (through teaching them to cross safely) and the road (by regulating cars, roads and town planning), so too with the former? Let us develop the analogy. In the case of road accidents, the risk to a child is defined as the probability of an accident x the severity of the consequences (anything from bruising to death). This is calculated by dividing the number of children hurt in various ways on the roads by the number of children in the population. Risk, harm, and the relation between them are as clear as the measurement of those two numbers is accurate.

But, on the internet, we do not know how many children come to harm. There are no accident figures. What we can measure, more or less, is how many children report crossing a road with cars on it. We don't know how many cars or how fast they are driving, and even more important, we don't know if an accident resulted. In the case of online pornography, for example, we have over a decade of surveys asking children if they have seen it but not, generally, exactly what they saw– and nor whether it harmed them. Recent efforts have got closer to exactly what happened – what they saw, what was said to them – in relation to pornography (Peter & Valkenburg, 2009), sexual harassment (Mitchell, Finkelhor, & Wolak, 2007) and cyberbullying (Smith, Mahdavi, & Carvalho, 2008).

But this is still to get a closer picture of what was happening on the road rather than what happened to the child. How, then, can we calculate risk? This is where the road analogy breaks down. Instead, we survey children who are online, ask how many encountered the 'risk' (i.e. that which carries a probability of harm), and divide the latter by the former. This means we report not the *'real risk*' (the probability of actual harm in the child population) but the *risk of the risk* (the probability of seeing pornography/receiving hostile messages/visiting a suicide chatroom etc); meanwhile the probability that this experience, in turn, will result in harm remains elusive. It's like reporting the risk of road accidents in terms of the likelihood of children crossing the road (albeit with increasing precision about the busyness of the road) rather than the risk of their being hurt. No wonder sceptics ask, so what, and policy makers are unclear about the implications for risk management.

Reflections on harm

> 'Physical or mental damage' (Merriam-Webster Dictionary)
> 'Material damage, actual or potential ill effect' (Oxford Dictionary of English)

The conditions under which risks (seeing online pornography, crossing the road) result in harm are complex, necessitating an analysis of *individuals* (themselves diverse, depending on life contexts) and of the socio-technical *environment* (behind which lie the institutions that shape them). Crucially, what we mean by harm is not always clear (Millwood Hargrave & Livingstone, 2009). For crossing the road, the harm is obvious. For seeing pornography, receiving hostile or sexual messages, visiting a self-harm chatroom or having your social networking profile trashed, what is the possible harm? This requires more discussion, surely,

but two kinds of harm are often implied. The first is *trauma* – an emotional response that indicates shock, distress, upset or sense of threat. The second is *damage*, physical or mental – encompassing being abused to low self-esteem, loss of friends, inability to form relationships, sexual problems or becoming aggressive to others.

By contrast with the emerging consensus on how to ask children about online risk, it is also less clear how to measure harm. Indeed, it is fairly commonplace to conclude that online harm experienced by children simply cannot be measured. Some therefore dismiss further consideration of the internet as affording children harm, along with the policy efforts to reduce such harm. Others draw the opposite conclusion. A strong position would be that all risk results in harm – for example, that any child who sees pornography or learns ideas of self-harm is in some way harmed (research ethics committees are inclined to take this approach). A weaker position asserts that certain risks surely result in harm - for example, a six year old exposed to hard core pornography. Whether a strong or weak position is taken, the *precautionary principle* is invoked to call for policy action in the absence of evidence (Klinke & Renn, 2001).

Two further approaches exist, both holding out hopes of evidence not only of risk but also of harm. One is to seek the equivalent of road accident statistics. 'Objective' evidence of harm might be expected from law enforcement, clinicians or child welfare services, for example, in cases where the internet is involved in incidence of sexual abuse or criminal abduction, youth suicide or self-harm attempts. But little such evidence has been forthcoming - possibly because the involvement of the internet is not reliably recorded in police or clinical records. Thus we know better how many children have gone to an offline meeting with an online contact, but not for how many this resulted in abuse. Nor, in the case of youth suicides, do we know the proportion of cases in which the internet played a role. Ten years after the advent of mass internet, we still rely on incidents learned of ad hoc, often from the media. And however many cases one hears of, it remains difficult to gauge what proportion of the population they represent.

The second approach to gaining evidence of harm is to ask children directly. Here researchers must rely on subjective methods - self-report surveys or interviews, asking children not only whether they have encountered pornographic or hostile messages, for instance, but whether it upset or bothered or distressed them. This can be valuable information in revealing how much risk does not result in harm: for example, up to half of the teenagers surveyed in studies reviewed by EU Kids Online had experienced various kinds of risk; but only about one in six said they had felt upset, threatened or distressed by their online experiences (Livingstone & Haddon, 2009).

However, this approach has its limitations too – there's much one cannot ask for ethical reasons, difficulties in establishing just what children mean by being 'upset'. Further, the resulting findings may not deflect the sceptics who ask whether a child can judge the harm done to them, especially as it may take years to be revealed, or even whether they are telling the truth. Nonetheless both these two approaches are worth pursuing further – and many researchers are engaged in either or both.

But let us return to the generally-compelling example of the six year old exposed to hard core pornography online. Why does such a case stimulate policy intervention even without direct evidence of harm? Because something is being implied about the child – a six year old is vulnerable. And something is being implied also about the internet – why is hard core pornography so readily available? This leads us first to the question of vulnerability, and

then to asking what difference the internet makes. These are the issues that should help us understand how measures of risk relate to the question of harm, in theory if not yet solidly in terms of evidence.

Reflections on vulnerability

In seeking to understand risk and its relation to harm, most researchers assume a complex set of contingencies mediate this relationship, together accounting for what makes some children more 'vulnerable' than others. Offline, though not yet online, the protective and risk factors that mediate the relation between childhood risk and harm have been well studied by child psychologists. Individual factors (for example, self-esteem, or socioeconomic status) may afford *protection* if they 'play a role in modifying the negative effects of adverse life circumstances and help to strengthen resilience' (Schoon 2006: 14; Schoon and Bynner 2003).

For example, higher self-esteem or higher status reduces the likelihood of harm, while their absence increases *vulnerability*. Over time, protective factors may build *resilience* in the individual while their absence further compounds *disadvantage*. Environmental factors may also increase protection or vulnerability – for example, the presence or absence of a positive school context or community support or good relations with parents. Note that risk factors may exacerbate both risk and harm in a similar fashion - lonely children are more likely to be bullied and more likely to be adversely affected if bullied. Or they may act in distinct ways – for example, boys are more likely to be exposed to pornography (i.e. a higher *risk*) but girls are more likely to be upset by such exposure (i.e. greater *harm*).

These points are uncontentious, yet as already noted, many studies examine the incidence of, say, hostile online messages received by children, without asking also if they are upset or harmed. Even when efforts are made to follow through from risk to harm, such contextual factors as family relations, self-esteem or socioeconomic status are rarely examined, and nor are questions asked about other circumstances in which the child may have been harmed or upset beyond those to do with the internet. And, last, even when all of these questions are investigated, the analysis may not be conducted to reveal the relation between risk and harm, the protective or vulnerability factors that influence that relationship, or a comparison between online and offline risk in order to judge the significance of the internet as a source of risk in children's lives.

What difference does the internet make?

In the offline domain, as already noted, the nature of risk and harm in childhood, the sources of vulnerability and resilience, and the effectiveness of different strategies of child protection and welfare are all well established and, if not fully understood, constantly developing. Can this knowledge simply be extended to understand vulnerability in the online domain? Should online risk be analysed in the *same* way as offline risk, and if not, what are the differences?

When reviewing findings from the first generation of internet studies, Woolgar (2002: 14-19) argued for continuities. He proposed five empirically-supported 'rules' for understanding developments in what he calls, with a deliberate question mark, the 'virtual society?', all of

which counter the popular assumption that the online and offline are quite distinct. Thus he observed:

- the importance of *contextualization* - 'the uptake and use of the new technologies depend crucially on local social context';
- the assumption of *inequality* - 'the fears and risks associated with new technologies are unevenly socially distributed';
- the consistent empirical evidence *against displacement* of the real - 'virtual technologies supplement rather than substitute for real activities';
- the counter-intuitive observation - '*the more virtual the more real*', since the growth of online activities/spaces has unexpectedly intensified, remediated or stimulated innovation in offline activities/spaces;
- *contra* claims about the death of distance, efforts to transcend the local and promote the global depend on specific local practices and identities - '*the more global the more local*'.

By contrast, the general argument that the internet introduces new experiences, risky or otherwise, is exemplified by boyd's (2008) claim that online communication is distinctively characterized by:

- *persistence* - being recorded (even permanent), thus permitting asynchronous communication (and long-term consequences);
- *scalability* - the considerable potential for visibility, rescaling simple interactions to constitute networked publics;
- *replicability* - enabling multiple versions with no distinction between the original and the copy (and, further, easy and seamless editing to manipulate content);
- *searchability* - permitting the easy construction of new, extended or niche relationships (including ready contact among 'strangers').

She adds that the dynamics of communication and social networking online are driven by three dynamics:

- *invisible audiences* - a radical uncertainty regarding who is attending to the communication (and, one might add, who is speaking) being built into the architecture of online spaces (exacerbated by conditions of *anonymity*);
- *collapsed contexts* – for the absence of boundaries impedes the maintenance of distinct social contexts;
- *public/private blurring* – this follows from the lack of boundaries and, when scaled up, has distinctive consequences.

As computer-mediated-communication scholars (Thurlow, Lengel, & Tomic, 2004) have argued, such features disembed communication from its traditional anchoring in the face-to-face situation of physical co-location, reembedding it in more flexible, more peer-oriented relations of sociability, thereby transforming the possibilities of communication for better or for worse. Distinctively, offline conduct is socially regulated by norms of behaviour and sanctions for their transgression. While online behaviour hardly goes ungoverned by social convention, the conventions are more flexible and less enforced in the absence of clear social cues, while the blurred boundaries no longer contain private interactions, enabling greater risk and risk-taking. And all this on a scale (in terms of physical and cultural distance, number of people and sheer amount of communication) that far exceeds the traditional limits, and established protective factors, of children's lives.

For these reasons, a review by ECPAT International for the United Nations concluded that the internet affords multiple opportunities for harm to children to a degree and in ways that did not previously exist (Muir, 2005). Thus for a child victim, an image of abuse may now be distributed anywhere worldwide in a matter of seconds and never eradicated. For the bullied child, a hostile site morphing their image and inviting ridicule may harm them whether or not they are aware of its existence. For a teenager in despair, a community of suicidal others, advocating the means of self-harm, may be reached at the click of a mouse with a convenience that is historically unprecedented. And for the young bully, racist or abuser, the creative potential of the internet invites new opportunities to harm others, unobserved and not easily detectable, even reaching into the privacy of their victim's bedroom (Livingstone, 2009).

Which of these positions is most useful for examining research on children's online risk? Is it that the children that are bullied in the playground are also bullied online, offline vulnerability sufficiently explaining online vulnerability? Or is it that children who, in their everyday environment, show no problems nonetheless encounter new risks online, diversifying the range of children at risk? Following Woolgar, one would expect evidence that children who are vulnerable offline are also vulnerable online (rule 1), that the adverse consequences of online risk are as unequally distributed as are offline risks (rule 2), and that far from providing an escape from offline difficulties, the online realm exacerbates this (rule 3) and feeds back so as to compound children's offline difficulties (rule 4); last, since more threats to children (from adults, from peers) come from known contacts rather than strangers, the global internet may also worsen local problems (rule 5).

An example of this comes from a recent UK survey of bullying among school children which found that, while 1 in 13 of 11-16 year olds are persistently cyberbullied, the incidence is higher among looked after children, children with special educational needs, the poor (those receiving free school meals) and ethnic minorities (Beatbullying, 2009). Moreover, two thirds of those who were persistently cyber bullied said this was an extension of offline bullying. Offline vulnerability seems to be extending its consequences online, as risk *migrates* from traditional to new sites.

The alternative possibility, *qua* boyd, would be that the internet affords new risks to children who may not previously have been at risk. What may most distress otherwise resilient children, thereby turning risk into harm, is the persistence of unwelcome or abusive content and conduct that, if offline only, could be quickly forgotten; also, once innocuous activities (such as giving personal details or photos to a friend) may be rendered newly harmful because of the searchability, replicability and manipulability of online content and identities. There is less research available that shows children to be newly at risk online. But there is growing research to suggest the internet reconfigures and exacerbates the experience of harm for those who are vulnerable.

An analysis of children who have actually been victimised online, from the UK's Child Exploitation and Online Protection Centre, shows that while one group, like that above, suggests risk migration, for it contained children who have already been sexually abused offline, a second group contained children who appear to have been randomly targeted by offenders through a range of social networking sites, chat rooms, online gaming , and so forth, and who share no apparent prior life circumstances. Possibly, these phenomena interact. The UK Children Go Online survey found that children and teenagers who were less satisfied with their lives

could, if they had online skills, feel more confident online than offline (Livingstone & Helsper, 2007). They valued the internet's potential for anonymous communication and the chance to exchange secrets or be silly or to disclose intimate aspects of their lives, and so were more likely to give out personal information, seek personal advice and make friends online and go to offline meetings with these new friends. In this case, offline disadvantage or dissatisfaction results in riskier behaviour which, given the specific affordances of the internet to compensate for or amplify the consequences of such behaviour, then compounds the risk. Crucially, one cannot conclude that, while the internet is fairly safe for most children its use should be more restricted for vulnerable children because it is in particularly for vulnerable or disadvantaged children that policy makers have such high hopes that the internet can provide a means of overcoming problems in the offline world (Bradbrook et al., 2008).

Since all children have offline experiences and most also have online experiences, we may identify four 'ideal types', perhaps real segments of the child population, perhaps some of them interacting with others.

		Online: *Resilient*	Online: *Vulnerable*
Offline	*Resilient*	**Most children?**	**New risks and/ or new risk-taking?**
Offline	*Vulnerable*	**Offline risk not extended? New opportunities?**	**Risk migration adds to vulnerability?**

Figure 2 Hypothetical relations between offline and online risk

The case of bullying can illustrate the table:

- Offline, most children are not bullied, able to stand up for themselves and/or lacking the vulnerabilities that lead other children to target them. If the internet makes little difference to the conditions of risk in children's lives, one would expect these children also not to be bullied online (or, if they are, for it to be relatively minor and not to result in much distress).
- However, it may be that the internet does make a difference, and that those children who are, or seem, resilient offline become somehow vulnerable online. Possibly they take new risks online, opening themselves up to attack in ways that they do not offline. Possibly too, different aspects of their identity are revealed online, making them either a random or a deliberate target for attack by others.
- For the minority of children who are bullied offline, a different set of conditions apply. If the internet makes little difference to these children, one would expect the bullying they experience offline to migrate online also, compounding their difficulties as the 'virtual' supplements the 'real' and the more 'virtual', the more 'real' also.
- But, instead, it may be that those who are bullied offline do not find an extension of their difficulties online. They may find a new way of presenting themselves, a chance to act differently online that can break the pattern and leave the 'real' behind. The online may even given them new opportunities – for advice and support, for developing coping strategies – that then helps them offline.

On the assumption that at least some children fall into each cell, a further set of questions arise which, together, could transform the knowledge base on children's online risk in ways that could guide future policy making.

1. *Descriptive knowledge*. How many children fall into each cell and what demographic or other characteristics (social, psychological, cultural, economic) discriminate among them? Are these stable classifications (since risks tend to be positively correlated with other, online and offline), or do children move between cells, or even fall into different cells for different risks?
2. *Risk migration hypothesis*. Given existing evidence on cycles of disadvantage, one may hypothesise that children in disadvantaged or 'at risk' life circumstances are more likely than those in 'normal' circumstances to be vulnerable offline. Do these same life circumstances shape their online experience, with the same risks migrating online, worsening matters offline in a vicious cycle?
3. *New risks?* If the risk migration hypothesis does not explain who experiences risks online, or if some children who experience risk online lack similar experiences offline, a key research question is, who are those newly at risk and why? Are their lives in some way more difficult than those who experience no risk online? Is their behaviour online different (e.g. particularly sensation-seeking)?
4. *New opportunities?* Is it possible that, for children who are vulnerable offline, the internet provides a safe haven, a space where risk does not follow them and new ways of acting can be developed? This research question raises another, namely, can these altered attitudes and behaviours even be transferred offline so as to build resilience and reduce offline risk?

Some further questions then arise:

5. *Children, or their life circumstances, as 'the problem'*. Is there a relation between vulnerability (offline or online) and perpetrating risks? One might hypothesise that the prior experience of offline risk (as a victim) leads some children (which?) to then become perpetrators (e.g. bullying others). Do adverse life circumstances lead some children to find online a new chance to take risks or attack others, even if such opportunities did not arise offline?
6. *The online environment as 'the problem'*. What are the specific affordances of different online products, services or platforms which enable or inhibit risk experiences? This may be asked descriptively: which risks are associated with which online activities (SNS, IM, chat, etc)? Or a set of hypotheses may be formulated: online risks will result when the child's identity is anonymous; when the site allows the easy adding of new contacts; or when search engines are provide risky answers to innocuous searches. Such questions and hypotheses should be sensitive to the continual and upcoming changes in the online environment.
7. *Minimising risk?* For children who experience risk neither offline nor online, what protective factors operate or what characterises them that might be encouraged in or taught to those in the three risk categories? For those in the three risk categories, what supports them or aids their rehabilitation, and can this be found online? In short, what would it take to move children out of the risk categories? Of the various solutions on offer – technological, education, awareness-raising, media literacy, parental mediation, regulatory and so forth – which are most effective in this regard, and for which children?

Complications

Three important problems are still unresolved by this analysis. The first is that the tripartite analysis of risk assessment, evaluation and management does not take into account the *benefits* of internet use, failing to balance opportunities against dangers. One may seek to avoid road accidents without stopping children cross the road. But it sometimes seems that for a child to avoid online risk, they can hardly do anything online: to post content online, you must provide personal details, to make new friends you must contact 'strangers', to explore diverse information may expose you to inappropriate content, to seek guidance on dieting will result in receipt of pro-anorexic advice, and so forth. As Livingstone and Helsper (2010) showed, children's take up of online opportunities is positively correlated with their exposure to online risk, with digital skills acting to increase the likelihood of both.

Unless children are to live in heavily filtered environments with Facebook and YouTube banned and adults always peering over their shoulders, a better resolution than a simple trade-off of opportunities and risks must be found. Pragmatically, this lends support the development of improved policies, parental and school mediation, media literacy and technical tools, so that one might hope to reduce risks without also reducing opportunities. To be sure such improvements are underway, but we should take note of a parallel domain, that of children's outdoor play. Here the supposedly improved tools of risk management (soft surfaces, safety rails, etc) have not, in practice, freed children to play as they would wish. Instead, an overly risk-averse culture has resulted that prevents children climbing trees or even swinging on swings without an onerous risk assessment undertaken by supervising adults (Gill, 2007).

This leads to a second complication – the particular sensitivities over risk evaluation in relation to *children*, for whom society finds it difficult to accept any degree of risk above zero. Shaped by the media's tendency to amplify risks, framing them as threatening the innocence of children (Kitzinger, 2004) and undermining the hope of an idealised, risk-free childhood (Kehily, 2010), for many parents risk anxiety has become 'a constant and pervasive feature of everyday consciousness' (Jackson & Scott, 1999: 88). There is, it seems, an unmanageable gulf between the rational balancing of probabilities matched to available policy tools and the unacceptability of harm that will still occur to a particular child. Although researchers and policy makers have learned to take great care in disseminating findings and recommendations to the media and public, this remains a difficult issue to be factored into any risk management strategy (Smillie & Blissett, 2010).

Third, and already foreshadowed in the above points, a world without risk is undesirable. Children must learn to take calculated risks and, insofar as is possible, cope with the consequences. Developmental psychologists are clear that facing and coping with risk is important, for 'resilience can only develop through exposure to risk or to stress' (Coleman & Hagell, 2007: 15). As Luthar, Cicchetti and Becker (2000: 543) define it, resilience is 'a dynamic process encompassing positive adaptation within the context of significant adversity.' The latter part of this definition is important – without experience of adversity, a child may be protected but has nothing to adapt to positively and so will not become resilient. A risk-averse society will, paradoxically, exacerbate rather than reduce the very vulnerabilities it seeks to protect by undermining the development of resilience. Lupton (1999: 156) adds that such dominant discourses as an excessive emphasis on safety generate their own counter-discourses: 'risk-taking may be regarded as the flipside of modernity, a response to the ever-intensifying focus on control and predictability of modernity' (the recent popularity of ChatRoulette illustrates the point).

Indeed, while even young children must, therefore, experience some degree of risk, for teenagers risk taking is also important developmentally and culturally. Teenagers are 'constantly engaged in risk assessment, actively creating and defining hierarchies premised upon different discourses of risk as 'normal' and acceptable or 'dangerous' and out of control' (Green, Mitchell, & Bunton, 2000: 123-4). They deliberately engage in what Hope (2007) calls 'boundary performances' – breaking the rules, taking risks, trying out new identities that transgress adult norms, as much in public as in private. For example, children hold lively conversations among themselves about the 'dirty old man' in the park or the 'weirdo in the chat room', for in this way they work out for themselves where their own agency and responsibility lies in engaging with a risky world (Willett & Burn, 2005). One would misunderstand the socialisation process to suppose that, once teenagers are aware of the risks they will cease to take them.

Conclusions

In terms of the analysis of risk and harm, it seems reasonable to conclude that it is useful to distinguish between *risk* (a calculation based on probability and the likely consequences of harm), and *harm* (a distinct outcome, whether measured objectively or subjectively). However, the field of children's online risk faces a particular problem in measuring harm, and therefore also struggles to measure risk, more often measuring the *risk of risk* – the nature and likelihood of particular risky experiences that bear an unclear relation to harm.

Online risk is rarely a *necessary cause* of harm, since few if any of the harms at stake are unique to the internet – all those on the public and policy agenda have a far longer history than the internet. Nor is online risk a *sufficient cause* of harm, since it may or may not result in a harmed child, depending on a host of factors to do with life circumstances (familial, psychological, socio-economic, life events, and many more) and immediate contextual factors (situation of exposure, presence of others, etc). To examine this, it is important to understand the *risk factors* that increase both risky experiences and the translation of risky experiences into harm - for some children or in some circumstances. *Protective factors* either prevent certain children from encountering risk or enable them to be resilient against harm when they do encounter risk. These factors must be researched in order to understand *when* risk results in harm, for *which children* this occurs, and whether the *same factors* that apply to offline risk also extend to online risk.

Does the internet make a difference? There is mounting evidence that children who vulnerable offline are also vulnerable online. There is also mounting evidence that the online environment exacerbates the experience of harm, though it is as yet uncertain whether it really transforms it. However, the task of responding to the *assessment* of risk (by first *evaluating* acceptable levels of risk and then developing policies to *manage risk*) is impeded by a public reluctance to accept any risk to children (notwithstanding growing public disquiet over a risk-averse culture of childhood) and, even more important, by the inability of risk calculations to take into account the *benefits* of internet use in general and of learning to cope with tolerable levels of online risk in particular.

Last, evidence of *benefits* as well as harms is needed to enable a proportionate balance between the opportunities and risks that the internet affords to children, recognising that the opportunities and risks often go hand in hand when using the internet and that striking this balance should be achieved differently for children who are more vulnerable or more resilient. In short, there can be no simple translation of online risks – or opportunities – into

predictable outcomes, and each can result in positive or negative outcomes for children, as shown in Figure 3 below.

Here the concept of internet affordances is valuable in reminding us that the internet is not intrinsically risky – everything depends on the interaction between users and their socio-technological environment, and the ways in which this interaction has been shaped. In some cases, online risks may *afford* harm (whether measured subjectively or objectively) but in others, they may facilitate resilience. Moreover, while online opportunities generally afford positive benefits for children, the existence of those same opportunities can, if children are restricted in accessing them, result in the negative outcome of digital exclusion.

	Internet Affordances		
Outcomes for children		*Opportunities*	*Risks*
	Negative	Digital (social) exclusion	Upset (subjective) Harm (objective)
	Positive	Benefits of internet use	Learning to cope (resilience)

Figure 3: Mapping internet affordances onto outcomes for children

Policy makers should, therefore, seek to address the challenges of online risk without increasing children's digital exclusion or leaving them vulnerable to harm. And that means taking action both improve design of the online environment and to enhance children's resilience.

References

Beatbullying. (2009). *Children's Online Risks and Safety*. London: Beatbullying.

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

boyd, d. (2008). Why youth ♥ social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, Identity, and Digital Media* (Vol. 6, pp. 119–142). Cambridge: MIT Press.

Bradbrook, G., Alvi, I., Fisher, J., Lloyd, H., Moore, R., Thompson, V., et al. (2008). *Meeting Their Potential: The Role of Education and Technology in Overcoming Disadvantage and Disaffection in Young People*. Coventry: Becta.

Coleman, J., & Hagell, A. (Eds.). (2007). *Adolescence, Risk and Resilience: Against the Odds.* Chichester: Wiley.

Feinstein, L., & Sabates, R. (2006). *Predicting adult life outcomes from earlier signals: identifying those at risk*: Prime Minister's Strategy Unit.

Finkelhor, D. (2008). *Childhood Victimization: Violence, Crime, and Abuse in the Lives of Young People.* Oxford: Oxford University Press.

Giddens, A. (1991). *Modernity and Self-Identity: Self and Society in the Late Modern Age.* Cambridge: Polity.

Gill, T. (2007). *No Fear: Growing Up in a Risk Averse Society*. London: Calouste Gulbenkian Foundation.

Green, E., Mitchell, W., & Bunton, R. (2000). Contextualizing risk and danger: An analysis of young people's perceptions of risk. *Journal of Youth Studie*s, 3(2), 109-126.

Hansson, S. O. (2010). Risk: objective or subjective, facts or values. *Journal of Risk Research,* 13(2), 231-238.

Hasebrink, U., Livingstone, S., Haddon, L., & Olafsson, K. (2009). *Comparing Children's Online Opportunities and Risks Across Europe: Cross-national Comparisons for EU Kids Online.* London: LSE, EU Kids Online.

Hope, A. (2007). Risk taking, boundary performance and intentional school Internet 'misuse'. *Discourse*, 28(1), 87-99.

Jackson, S., & Scott, S. (1999). Risk anxiety and the social construction of childhood. In D. Lupton (Ed.), *Risk* (pp. 86-107). Cambridge: Cambridge University Press.

Kehily, M. J. (2010). Childhood in crisis? Tracing the contours of 'crisis' and its impact upon contemporary parenting practices. *Media, Culture & Society*, 32(2), 171-185.

Kitzinger, J. (2004). *Framing Abuse: Media Influence and Public Understanding of Sexual Violence against Children*. London: Pluto Press.

Klinke, A., & Renn, O. (2001). Precautionary principle and discursive strategies: classifying and managing risks. *Journal of Risk Research*, 4(2), 159-174.

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

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

Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final Report*. London: London School of Economics and Political Science, Department of Media and Communications.

Livingstone, S., & Helsper, E. (2010). Balancing opportunities and risks in teenagers' use of the internet: The role of online skills and internet self-efficacy. *New Media & Society,* 12(2), 309-329.

Livingstone, S., & Helsper, E. J. (2007). Taking risks when communication on the Internet: The role of offline social-psychological factors in young people's vulnerability to online risks. *Information, Communication & Society*, 10(5), 619-643.

Lupton, D. (Ed.). (1999). *Risk*. London: Routledge.

Millwood Hargrave, A., & Livingstone, S. (2009). *Harm and Offence in Media Content: A Review of the Empirical Literature* (2nd ed.). Bristol: Intellect Press.

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007). Online Requests for Sexual Pictures from Youth: Risk Factors and Incident Characteristics. *Journal of Adolescent Health*, 41(2), 196-203.

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

Munro, E. (2008). *Effective Child Protection* (2 ed.). London: Sage.

Peter, J., & Valkenburg, P. M. (2009). Adolescents' Exposure to Sexually Explicit Internet Material and Notions of Women as Sex Objects: Assessing Causality and Underlying Processes. *Journal of Communication*, 59(3), 407-433.

Schoon, I. (2006). *Risk and resilience: Adaptations in changing times.* New York: Cambridge University Press.

Smillie, L., & Blissett, A. (2010). A model for developing risk communication strategy. *Journal of Risk Research*, 13(1), 115-134.

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

Thurlow, C., Lengel, L., & Tomic, A. (2004). *Computer Mediated Communication: Social Interaction on the Internet*. London: Sage.

Valkenburg, P., & Peter, J. (2007). Preadolescents' and adolescents' online communication and their closeness to friends. *Developmental Psychology*, 43(2), 267-277.

Willett, R., & Burn, A. (2005). 'What exactly is a paedophile?': Children talking about Internet risk. *Jahrbuch Medienpädagogik*, 5, 237-254.

Woolgar, S. (2002). Five rules of virtuality. In S. Woolgar (Ed.), *Virtual Society? Technology, Cyberbole, Reality* (pp. 1-22). Oxford: OUP.

Ybarra, M. L., & Mitchell, K. J. (2008). How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. *Pediatrics,* 121, e350-e357.