INTERNET SAVVY? CHILDREN AND ONLINE RISK

LELIA GREEN

Professor of Communications
School of Communications and Arts
Edith Cowan University
Perth, Western Australia

Abstract

Over the past five years there has been an explosion of research into the risks that (particularly) children run when they interact online. EU Kids Online I ran from 2006–09 and assessed over 400 studies drawn from 21 EU countries before moving into a new phase (EU Kids Online II) with comparative research across 25 European nations with a budget of 2.5M Euro.

In the United States, the Internet Safety Technical Task Force deliberated throughout 2008 before issuing a final report at the end of that year which particularly addresses the risks run by children’s activities on Social Network Sites such as Facebook.

In Australia, the major ACMA report on Media and Communications in Australian Families (2007) has been supplemented by four shorter research reports considering specific aspects of media use by young people and in family groups; and three annual reports examining online risk and safety more broadly (2008, 2009 and 2010).

This research indicates that children’s risk taking is across a range of contexts; deemed by the EU Kids network to encompass Content, Contact, Conduct risks. Risk taking varies with gender and age, and with the relative prevalence and uptake of the internet in the society concerned. Not all risk confers harm, however, and as well as reviewing key aspects of the research discussed here, the paper suggests that policy makers also have a responsibility to address children’s perceptions of discomfort and harm as a result of their internet activities, and their coping strategies and relative resilience. Since this paper was proposed the ARC Centre of Excellence for Creative Industries and Innovation has commissioned research to parallel EU Kids Online II, which will allow some benchmarking across 26 nations, including Australia.

Paper

As the internet has become more pervasive, in terms of the amount of tasks and activities it is used for, and in terms of the amount of time for which it is used, so have fears about children’s use of the internet also increased. Indeed these fears, at least in advanced economies, have generally replaced fears about equity of access and the relative digital divide. This paper compares fears about risks with the lack of established knowledge about harm, and suggests that a realignment of priorities is in order.

Recent research by the Australian Communications and Media Authority (ACMA) indicates that 91 per cent of all families with children aged 8–17 have internet access, and this figure is ‘higher in family households with 14–17-year-olds (96 per cent)’ (ACMA 2008b, p. 23). Around the world, government responses to young people’s participation in online activities have included the commissioning and completion of a range of far-reaching research projects. In Australia, the landmark report Media and Communications in Australian Families was released in 2007 (ACMA 2007), and followed up by four shorter reports (ACMA 2008a; b; c; d). In the States, the Internet Safety Technical Taskforce reported at the end of 2008, in their Enhancing child safety and online technologies (ISTTF 2008) report. In the EU, in 2009 in the grip of the global downturn, the European Commission’s Safer Internet Program allocated €2.5M for a research project dubbed

© Lelia Green 226
EU Kids Online II. This arose out of the previous three years’ long EU Kids Online project which had run from 2006–09, now termed EU Kids Online I, and which had examined some 400+ robust research projects investigating children’s internet use, carried out in the EU, to identify lessons learned and the gaps in the research record with a view to informing future policy and practice in the area (Livingstone & Haddon 2009).

In addition to government desires to collect detailed information about children’s online activities, concern over this topic is a prompt for much discussion in the media, and particularly in newspapers. Haddon and Stald (2009) examined the content of press stories about children and the internet in 14 European Union (EU) countries over the two months of October–November 2007. Although data from Bulgaria was not included in the section of the paper dealing with content analysis, due to the small number of Bulgarian stories, twelve of the remaining thirteen countries had the highest percentage of children and internet content codes in the ‘Legal/Crime/Police’ categories. In eight countries, this category was not only the largest one, but contained more than half of all stories circulating about children’s use of the Internet. Denmark was the sole exception to this ‘Legal/Crime/Police’ focus, with 81% of (comparatively fewer overall) stories categorised in the ‘Entertainment/Play/Leisure’ codes.

In the face of these discourses, which over the course of the case study tended to highlight risks and minimise benefits, it was left to advertisers and marketers of digital goods and services to emphasise the positives. Internet researchers often feel the need to restate the generally beneficial nature of children’s online activities as a corrective to the predominantly negative discourse of risk in the public sphere: ‘children use the internet as an educational resource, for entertainment, games and fun, for searching for global information and for social networking, sharing experiences with distant others’ (Hasebrink et al. 2008, p. 25). However, such researchers also acknowledge that there is risk in some children’s online interactions and they work hard to understand its relative pervasiveness and severity.

Recent Australian initiatives to address children and risk

There has been considerable attention paid at home and abroad (Moses 2010a) to the possibility of Australia’s introduction of a mandatory internet service provider (ISP) filter (Lumby et al. 2009). This interest has been further fuelled by the debate on an expanded ‘refused classification’ category which would inform the compulsory blocking of prohibited sites (Moses 2010b). As indicated in the Wikileaks’s revelations concerning the August 2008 ACMA blacklist, and the government’s response, the number of sites affected in that period was somewhere between 1061, the Conroy figure (MacBean 2009) and 2395, the number of sites in the Wikileaks exposé (Moses 2009). Moses comments that:

about half of the sites on the list are not related to child porn and include a slew of online poker sites, YouTube links, regular gay and straight porn sites, Wikipedia entries, euthanasia sites, websites of fringe religions such as satanic sites, fetish sites, Christian sites, the website of a tour operator and even a Queensland dentist. (Moses 2009)

The ISP filter proposal, which is still active according to some reports (Moses 2010c), is designed to catch material which includes child sexual abuse sites, rather than the everyday pornography which might be of particular concern to parents. It follows a range of more modest government initiatives from the mid-2000s onwards. Often branded as an anti-porn programme, the NetAlert — Protecting Australian Families Online safety initiative took shape in 2007 in the last months of the third Howard Government, with a national media and public education campaign in September 2007 which included a booklet delivered to every Australian household, extensive web resources and the launch of a specially created free internet filter product, NetAlert (Best 2007a). The government expected 2.5M households to download the filter but fewer than 150,000 households did so (Gilmore 2008). A 16-year-old school boy, Tom Wood, cracked the filter in just over 30
minutes, and cracked the upgrade in 40 minutes (Best 2007b). Web tutorials on how to bypass the filter were posted onto *YouTube*, although these soon had over-18 restrictions placed on them.

In December 2007 ACMA released its extensive report based upon in-depth qualitative research which informed telephone interviews with parents in 751 families and self-completed diaries from 1003 children aged 8–17: *Media and Communications in Australian families 2007*. The research demonstrated that most Australian parents use a range of strategies to mediate their children’s online activities, and that parental concern and regulatory approaches change with the age of the child (ACMA 2007, pp. 126–7), and with gender (ACMA 2007, p. 95). Parents have household rules and regulations; they use social approaches and talk with their children about what they are doing and what they see online. Some also use technological tools such as filtering and monitoring web histories:

Most parents trust their child’s judgement about the internet and, at least some of the time, leave it up to him/her to choose what is done on the internet (83 per cent). This includes two-thirds who trust their child’s judgement all/most of the time (66 per cent). Nonetheless, most households (75 per cent) have rules, understandings or arrangements (ACMA 2007, p. 28).

Although generally supportive of their child’s online activities, studies such as those by ACMA (2007) and Ito et al. (2008) indicate that parents are increasingly struggling to control their children’s media activities. Social networking, blogging, video-sharing sites, online games and mobile digital devices such as iPods and phones are key elements of Web 2.0 youth culture, providing opportunities for communication, friendship, play, and self-expression that may not be fully understood or totally controllable by parents (Green 2010, pp. 93–7). Indeed, parents may have a range of concerns about the amount of online activity in which their child engages and/or the kinds of activities chosen, hence the rules and understandings developed in the home that parents hope will govern, or influence, internet use.

**Do parents and children agree about online risk?**

Even with some shared understanding or arrangements about children’s domestic access to the internet, in Australia and internationally, parents and children disagree over whether there are household rules regarding the Internet, and what these rules may be. For instance, a NetRatings (2005) survey of 410 Australian parents and 502 children found that 7% of children perceived their family as having no rules at all regarding internet use, while all parent respondents reported that they had internet-use rules in place. (0% of parents said there were no rules.) The 2007 ACMA report, reviewing Australian research on rule-setting, finds that there ‘is a large and statistically significant difference in parents’ and children’s reporting of both rule setting and parental supervision activity, with children reporting less supervision and rule-setting’ (2007, p. 289). This is borne out in EU research where children report fewer family-based rules around internet use than do their parents; while parents report that their children have less exposure to online risks than their children say they do (Livingstone & Haddon 2009, p. 28).

One rationale offered for these discrepancies is that parents may wish to be seen by researchers as ‘good care-givers’ and overstate their rule-setting; while children may not understand the rules that their parents have put in place, or may see them as inconsistently applied and thus discount or underestimate them. Alternatively, the child’s denial of such rules may be ‘a tactic to evade restrictions on access to pleasurable content and activities, particularly private communications with peers’ (ACMA 2007, p. 298). Nonetheless, it is clear that the home is central to children’s safe use of the internet: not so much in the rules that the parents lay down, but in the child’s safe and healthy development offline. Reviewing the available literature, the large-scale US report *Enhancing child safety and online technologies* argues that: ‘Depression, abuse and substances are all strongly correlated with various risky behaviours that lead to poor choices with respect to online activities. A poor home environment that includes conflict and poor parent–child relationships is correlated with a host of online risks (Wolak et al. 2003; Ybarra & Mitchell 2004).’ (ISTTF 2008, p. 20)
Adults and children worry about different aspects of children’s web use. Children worry about cyber bullying, identity theft and spam (Livingstone & Haddon 2009, p. 51). Adults worry about pornography, stranger danger and access to online information about self-harm, suicide and anorexia (Livingstone & Haddon 2009, p. 27). Interestingly, the higher the percentage of families online in a country, and the more that parents are experienced themselves in the online environment, the less concern they report. However, if parents are internet users, they report more mediation of their child’s internet use; non-using parents mediate less (Livingstone & Haddon 2009, p. 27). Further, within countries, ‘even though higher status parents are more likely than those of lower status to provide their children with access to the internet, this [thus] generally enabling more use among advantaged children, it seems that lower class children are more exposed to risk online’ (Livingstone & Haddon 2009, p. 23). Thus risk appears reduced where parents are also active online and it is not necessarily lessened by restricted access to the internet.

Increasingly research indicates that children who are at risk online are likely to be the children who are at risk overall. These risk-prone children include those who are in conflict with their parents, or depressed; and children whose lives are affected by drink, drugs, and poor relationship skills. Wolak et al. (2008) argue that ‘particular attention should be paid to higher risk youths, including those with histories of sexual abuse, sexual orientation concerns, and patterns of off- and online risk taking’. Those children most at risk online include those most likely to lack parental interest and involvement. A landmark project in Australia funded through the Telstra Foundation, is working with such children with the aim of raising ‘awareness within the sector and among policy-makers and funding bodies about the benefits of access & equity to technology for vulnerable children & young people’ (Oliver 2010, p. 5).

Livingstone and Haddon (2009, p. 39) note that addressing ‘the risks faced by a vulnerable minority in a proportionate manner without extending undue surveillance and restrictions to the occasionally naïve, sometimes risk-taking majority is undoubtedly a difficult problem for public policy.’ This problem is exacerbated in that risk is related to children’s age, gender, socio-economic/educational status and cultural contexts and cannot necessarily be dismissed as straightforwardly negative. In particular, it has been argued that children learn resilience through their negotiation of risk (Livingstone & Haddon 2009, p. 34). Many older children will deliberately engage in risky behaviour and ‘children may be expected to circumvent, evade or subvert adult expectations or norms for their behaviour’ (Lobe, Livingstone & Haddon 2007, p. 17). Older Australian children, for example, are less likely to follow parental injunctions to use the internet according to the recommended Cybersmart (n.d.) protocols.

Responsible risk-taking has been associated with the desirable characteristics of innovative behaviour. The UK’s National Endowment for Science, Technology and the Arts (NESTA) has published a research report arguing that ‘five generic skills [...] underpin innovative behaviour and form a set of attributes clearly linked to the innovation process’ (Chell 2009, p. 4). These attributes are: creativity, confidence, energy, risk-propensity and leadership. ‘Risk-propensity’ is defined as being ‘a combination of risk tolerance and the ability to take calculated risks’ (Chell 2009, p. 4). Such awareness of risk, and the capacity to take calculated risk, is developed through progressive exposure to risk and review and reflection upon risk-taking behaviour. Arguably, the structured development of risk-awareness underpins the evolving mediation schemes within the family that ACMA reports Australian parents adopting with their children; varying their supervision and regulation strategies as the child matures (ACMA 2007, 117–20).

Accordingly, instead of attempting to mandate general risk-avoidance, evidence-based policy should concentrate upon the minimisation of actual harm. EU research indicates that between 15–20% of teens self-identify feeling distress, discomfort or threat as a result of what they have encountered online (Livingstone & Haddon 2009, p. 23), although a much greater proportion of teens engage in ‘risky’ behaviour. 50% have revealed personal information online; 40% have seen pornography; 33% have been exposed to violent images or hate sites; 20% have been bullied online
and 9% have met strangers that they first contacted in an online environment (Livingstone & Haddon 2009, p. 3).

Considering the nature of online risk

As a result of examining some 400+ European research projects investigating children’s online activities, the EU Kids Online I project categorised the risks children run as being one or more of conduct, contact and content risk. According to Hasebrink et al. (2008, p. 8):

1. **Conduct risks** are where the child is the actor, offering content or acting in personal contexts. These risks include activities that reveal personal identifying information enabling others to contact and possibly harm the child; copyright-infringing downloads; and recognise that children themselves may be the major perpetrators of risks that other children encounter.

2. **Contact risks** are where the child is a participant in peer or personal communication. The implications of this risk category include the possibility that a child will choose to meet in real life someone they have got to know online.

3. **Content risk** are where the child is the recipient of mass communication and include children’s exposure to pornography; hate sites; gambling; self-harm, suicide and anorexia sites.

The researchers note (Hasebrink et al. 2008, p. 8) that ‘issues of privacy and personal information cut across cells’ and ‘some categories [of motivation] (e.g. sexuality) cover rather different kinds of risk’.

Livingstone and Haddon report that boys are more likely to experience, or create, conduct risks, while girls are more prone to content and contact risks. In particular, boys are:

- more likely to seek out offensive or violent content, to access pornographic content or be sent links to pornographic websites, to meet somebody offline that they have met online and to give out personal information. Girls appear more likely to be upset by offensive, violent or pornographic material, to chat online with strangers, to receive unwanted sexual comments and to be asked for personal information although they are wary of providing it to strangers. Both boys and girls appear at risk of online bullying. (Livingstone & Haddon 2009, pp. 23–4)

It is only recently that researchers have begun investigating the possibility, which is now supported by significant evidence, that many of the incidents children find most distressing are perpetrated by other children. Hasebrink et al. (2008, p. 32) categorise this research as mainly focussing on children as perpetrators of bullying behaviour and as the senders of unwanted sexual messages. Wolak et al. (2007) report that ‘nearly all (99%) of Internet-initiated sex crime arrests in the N-JOV study [a US national dataset] were aged 13–17’ (cited in ISSTF 2008, p. 19). Although parents remain concerned about cyber predators and online grooming, and although a number of regulatory initiatives have targeted these fears (Green 2009), studies indicate that today’s children may actually be at significantly less risk of sexual assault than they were in the early 1990s. Finkelhor’s view (2008) is that ‘the −53% [minus 53%] change in reports of sexual offences against children from 1992 to 2006 […] is both significant and real’ (Schrock & boyd 2008, p. 10). There is little research to explain why a decline in US reports of sexual assaults against children might parallel the rise of the World Wide Web, but this absence reflects the fact that discussion of internet risk usually fails to connect online experiences with events in the offline world.

Research is less likely to focus on maximising possible benefits of children’s use of the internet than on minimising risk. Further, policy formation around reducing online risk generally fails to engage with the problematic that internet opportunities and benefits may be curtailed through mandating a restrictive online environment. One exception to this generalisation about research is offered by Hasebrink et al. (2008). Hasebrink’s report provides a counterpoint to the discussion of risk by also considering opportunities. The potentially negative consequences of activities motivated by commercial interests, aggression, sexuality and challenging values/ideology (2008, p. 9) are explicitly balanced in comparing children’s online opportunities and risks across Europe by
discussion of possible positive consequences of using the internet for education and learning, participation and civic engagement, creativity, identity and social connection (2008, p. 10). Given it appears that children at greatest risk online are also those at most risk offline (Hinduja & Patchin 2007; Ybarra et al. 2007), such children deserve multi-faceted policy and intervention supports in addition to paying attention to maximising a sense of social inclusion and possible benefits flowing from their internet activities (Oliver 2010).

Do we know what makes for children’s savvy internet use?

The ideal outcome to result from the mediation of children’s online engagement is that the child matures into a competent, creative, innovative, internet-using adult. Such an outcome is unlikely to be facilitated through legislated measures to address risk. Research indicates that savvy internet use is promoted by responsible risk-taking and decision-making as the child matures, combined with the development of a range of internet-related skills and competencies. The changing environments of internet access mandate the development of widespread internet-savvy skills. This approach is particularly apt as a result of children using mobile phones and newer technologies such as iPads to access social networking sites and other online properties. Remote access obviates many home- and school-based controls and supervision strategies designed to ensure responsible internet use (ACMA 2007, pp. 117–20). Hitherto, parents’ concerns might have centred on the more or less lax approach to internet access adopted by other households that their children might visit, or on offer in internet cafes. Parents today have to take into account that educating their child about online activities is the most portable safeguard protecting them against troubling internet interactions. Education and informed decision-making are key aspects of savvy internet use.

Apart from accepting this approach, which is one of the arguments against the introduction of a mandatory filter which may make parents feel that their children are protected from troubling content when they are not, we know very little about whether Australian children are savvy internet users. We are also unclear as to the key behaviours that relate to the online experience of harm, as opposed to risk. What is required is systematic research that links: online risk-behaviour to perceptions of actual harm; online risk-taking to troubling offline behaviours such as abuse, violence, drug use and poor parent–child relationships; and online risk-taking to psychosocial characteristics. Detailed research along these lines is yet to be carried out in Australia. The Australian Internet Industry Association has called for such research in its 2010 Manifesto: ‘it is essential that more local research is undertaken to provide a credible evidence base for future policy work. There is a central role for Government in supporting such research so that the goal of evidence-based policy is realised’ (IIA 2010, p. 44). The Australian government is yet to respond by funding research that puts the child at the centre of evidence collection, continuing instead to survey parents and teachers about children’s activities (DBCDE personal communication, May 2010).

The European Union has been more proactive. As the EU Kids Online projects I and II indicate, the EU regards this research agenda as critical to promoting the digital future. The EU Kids Online II research network has almost completed surveying 25,000 children aged 9–16, and 25,000 parents and care-givers (the parent most responsible for the child’s online activity), across 25 nations including Norway and Turkey. The national sample for each of the 25 countries involved constitutes 1,000 children plus 1,000 parents, recruited according to principles of random selection. The survey work itself is carried out by experienced market researchers, all internationally affiliated with the IPSOS organisation to promote consistency of approach and comparability of results, in face to face contexts in the home.

In the EU kids Online II research, the parent is surveyed separately from the child to assess, for example, whether there are shared understandings of household rules, and shared perceptions of whether the child has been distressed by material on the internet in the past year and, if so, what s/he found distressing and how long s/he was distressed for. Parents are also asked about their child’s social networks and the things they worry about ‘a lot’ in relation to their child, such as: school
performance, bullying, drug and alcohol use, sexual activity, getting into trouble with the police: as well as aspects of the child’s internet activity. This allows some contextualising of parents’ fears around internet use. The parent is also asked about their own internet use and their mediation practices around their child’s activities and time online.

The child in the family with the next birthday is the representative child of that family surveyed; provided they are aged between 9–16 and provided they have been online in any location at some point in the previous 12 months. All children are asked questions about where they go online, family rules about internet use, what they do online (in terms of chat, using webcam, filesharing, posting images etc. Their online competencies are also assessed through these questions. When it comes to risks, children aged 9and 10 are asked fewer questions and on a more restricted range of subjects than are the 11–16-year-olds.

All ‘personal’ questions to child respondents, such as about drug use, trouble with the police, sexual activity, and the perpetration of bullying are self-completed by the child in the presence of the surveyor but in privacy, without the surveyor being able to see what the child responds. Answers to these questions allow the child’s risk taking behaviour and experience of harm online to be placed in a context of risk-taking behaviour and the experience of harm offline. The research addresses the need to link online activity with the child’s psychosocial characteristics to maximise the relevance of evidence-based policy to address internet harm. While the child responds to personal ‘self-completion’ survey questions the surveyors role, as required, is to explain context and language use, especially around the notion of ‘being bothered’. The notion of being bothered by something is critical since it aims to capture the feeling of being unsettled, as well as being distressed.

Not all children answer all parts of the survey. Specific sections of the survey are triggered by previous responses which indicate the child has been bothered by something they have encountered on the internet, or through their internet use, in the previous twelve months. Having established that the child has been bothered by one or more of bullying/being bullied, seeing sexual images, and challenging content (self-harm, suicide, anorexia, hate-sites, drug use), data on these experiences are gathered in the context of both online and offline exposure. This puts online bullying in the context of offline bullying, for example; and pornography online in the context of exposure to pornography offline.

Children are also asked if they have used the internet for social purposes, and if they have placed personal information on the internet (as specified), and if they have met new people online that they have then met offline and, if so, whether they were bothered by any aspect of the encounter. Similar questions are asked about sexting on the internet: whether they have sent sexual messages (words, pictures or videos) of themselves, or received sexual messages from another person, and if that behaviour had bothered them. If a child has been bothered by any experience on the internet, the relative distress is investigated by asking whether they were upset and to what extent (from ‘not at all upset’ to ‘very upset’), and for how long the feeling lasted (‘I got over it straight away’ to ‘I thought about it for a couple of months or more’). The child is also asked about their coping strategies: what they did, who they spoke to (if anyone) and how they changed their internet use (if at all). These questions investigate resilience and personal knowledge about available blocking strategies; as well as risk exposure and any harm experienced by the child.

Conclusion

Although there has been significant legislation around the globe to protect children from risks online, there has been little robust research to inform evidence-based policy. Such policy should place children’s online risks in the context of children’s offline risks and assess children’s experience of harm and the extent of that harm. There have also been few explicit attempts to balance risk reduction strategies against possible implications for reducing online opportunities and competencies. Informed regulation in such a complex area cannot occur without detailed and nuanced research.
In Europe, the EU Kids Online II project will provide robust benchmarking data and evidence to inform nuanced policy for 25 nations including many leading OECD economies. Australia was offered an opportunity to be ‘country 26’, but the government at that time had already expended its Cybersafety budget and was committed instead to researching the opinions of parents and teachers as to children’s safety online. Given that timing is crucial if Australia is to participate in benchmarking with 25 European nations, the ARC Centre of Excellence for Creative Industries and Innovation (CCI) has commissioned IPSOS Australia to survey 400 children and 400 parents; the maximum number affordable by the CCI. For the research to be truly comparable with that carried out in the other 25 nations, however, more funds are urgently required to pay for the surveying of a further 600 children and 600 parents, and to support data analysis and reporting prior to the datasets entering the public domain (in 2012).

Discussions around children’s online activities need to move on from a predominant emphasis on risk and safety. Regulatory frameworks need to recognise explicitly the value of confident internet skills for the innovation economy, and the imperatives of digital citizenship. Insofar as harm is a focus, researchers need to know more about what promotes resilience, coping and the reduction of harm rather than concentrating on minimising risk. It will also be valuable to understand how harm relates to general patterns of abuse, substance misuse and deprivation, and specific guidelines for children living with these challenges. Australia almost missed the opportunity to be included in the research project which is best placed globally to address these issues and it is to be hoped that other parties will join CCI to help ensure that Australia’s work in this area is not too little, too late.

REFERENCES


Green, L. (2009). Minors online and their risks from cyber predators: Should we protect or empower? *COST298 The good, the bad and the challenging*, Conference proceedings, Copenhagen, Denmark, 13–15 May, pp. 283-89.


