Research Review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age

Sonia Livingstone
Department of Media and Communications, London School of Economics and Political Science, London, U.K.

Peter K Smith
Unit for School and Family Studies, Department of Psychology, Goldsmiths, University of London, U.K.
Abstract

**Aims and scope:** the usage of mobile phones and the internet by young people has increased rapidly in the past decade, approaching saturation by middle childhood in developed countries. Besides many benefits, online content, contact or conduct can be associated with risk of harm; most research has examined whether aggressive or sexual harms result from this. We examine the nature and prevalence of such risks, and evaluate the evidence regarding the factors that increase or protect against harm resulting from such risks, so as to inform the academic and practitioner knowledge base. We also identify the conceptual and methodological challenges encountered in this relatively new body of research, and highlight the pressing research gaps.

**Methods:** given the pace of change in the market for communication technologies, we review research published since 2008. Following a thorough bibliographic search of literature from the key disciplines (psychology, sociology, education, media studies and computing sciences), the review concentrates on recent, high quality empirical studies, contextualising these within an overview of the field.

**Findings:** risks of cyberbullying, contact with strangers, sexual messaging (‘sexting’) and pornography generally affect fewer than one in five adolescents. Prevalence estimates vary according to definition and measurement, but do not appear to be rising substantially with increasing access to mobile and online technologies, possibly because these technologies pose no additional risk to offline behaviour, or because any risks are offset by a commensurate growth in safety awareness and initiatives. While not all online risks result in self-reported harm, a range of adverse emotional and psychosocial consequences is revealed by longitudinal studies. Useful for identifying which children are more vulnerable than others, evidence reveals several risk factors: personality factors (sensation-seeking, low self-esteem, psychological difficulties), social factors (lack of parental support, peer norms) and digital factors (online practices, digital skills, specific online sites).

**Conclusions:** mobile and online risks are increasingly intertwined with pre-existing (offline) risks in children’s lives. Research gaps, as well as implications for practitioners, are identified. The challenge is now to examine the relations among different risks, and to build on the risk and protective factors identified to design effective interventions.

**Keywords:** cyber aggression bullying internet online mobile pornography sexual risk harm protective child
The rapid growth in development, accessibility and use of mobile phones and the internet has transformed the lives of most people, especially in developed countries, throughout the early years of this century. Children and young people who have grown up with these innovations are popularly dubbed the ‘digital natives’ of a changed communication landscape that is still evolving and only partially understood (Prensky, 2001), and has been referred to as a ‘techno-microsystem’ (Johnson, 2010). Absorption in online communication, followed by use of smart phones and social networking, has been seen as typical of adolescents, but it is becoming characteristic of ever younger children. Mobile and online technologies have brought enormous opportunities for pleasure and communication, knowledge seeking and exchange. But they also bring risks, including cyberbullying, contact with strangers, sexual messaging (‘sexting’) and pornography. These are periodically the subject of considerable public concern among parents, educators and clinicians, as amplified by the mass media (Ling & Haddon, 2008; Vandebosch, Simulioniene, Vermeulen, Marczak & Bonnetti, 2013).

Partly in response, a new and multidisciplinary field of research has emerged over the past two decades, with specialist journals being established, such as *Journal of Computer-Mediated Communication* (1996-), *Cyberpsychology, Behavior, and Social Networking* (1998-), *New Media & Society* (1999-), *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* (2006-), *International Journal of Cyber Society and Education* (2008-), as well as older journals turning their attention to online risks to children, such as *Computers in Human Behavior* (1984-) and special issues of major disciplinary journals in psychology, sociology, education, media studies and computing sciences. Major studies have been conducted in the US by the Pew Research Center, the Crimes Against Children Research Center, and the Berkman Center for Internet & Society, and by the EU Kids Online network in Europe, and COST Action IS0801 on cyberbullying in Europe and Australia.

This review examines the evidence for aggressive and sexual harms associated with online and mobile content, contact and conduct, with the focus on minors (under 18 years old). With the primary aim of informing the academic and practitioner knowledge base, our interlinked objectives are to identify the types and prevalence of these risks of harm to children, bringing together the literatures on diverse types of harm, and then to reveal the factors that increase or protect against risks. Most research, and our present focus, centres on victims rather than perpetrators of harm, although the line between the two is blurred, and some children fall into both categories. A secondary aim is to identify the conceptual and
methodological challenges encountered in this relatively new body of research, and to highlight the pressing research gaps.

The article is organised as follows. First, we briefly review the rapid growth in children’s access to mobile and internet technologies. Then we set out the methodology for our review, noting some methodological limitations of the field. We have sought to distinguish research focused on the evidence for risk (a calculation based on probability and the likely consequences of harm, and usually studied in terms of exposure to potentially harmful phenomena such as pornography or hostile messages) from that which examines harm (a distinct and negative outcome, whether measured objectively or, more usually, through subjective self-report) (Klinke & Renn, 2001; Millwood Hargrave & Livingstone, 2009; Schoon, 2006). We examine the definition, nature and prevalence of first aggressive and then sexual risks associated with the use by adolescents of the internet and mobile phones. These findings are further examined for comparisons across individuals (by age and gender), across countries (with most research concentrated in Europe, North America and Australia) and over time (particularly, the past fifteen years in which online and mobile technologies have become widely used in developed countries). Although there is less available longitudinal research on the harm that results from online risks, this is reviewed next. Finally, we examine the evidence for risk and protective factors (individual, social, environmental, and technology-related) that affect adolescents’ exposure to risk of harm, before drawing conclusions for future research and for practitioners working with children.

The growth of mobile and internet usage among children and young people

Across the world’s wealthy countries, the trend is for media and communication devices to become internet-enabled and portable. While household saturation in internet and telephony was reached some years ago, personal ownership of multiple devices continues to rise. Insofar as this includes the provisioning of children, internet and mobile use is becoming more private and inaccessible to parental oversight (Livingstone, 2009). UK figures for 2012 show that internet use at home is strongly age-related: 37% of 3-4 year olds, 58% of 5-7 year olds, 87% of 8-11 year olds and 95% of 12-15 year olds (Ofcom, 2012). Further, half of 5-15 year olds have a mobile phone: 6% of 5-7 year olds, 43% of 8-11 year olds and 87% of 12-15 year olds. The proportion of these phones that are smart phones increases with age, rising to 62% of all 12-15 year olds, as does ownership of other smart devices (tablets, games consoles, music players).
Figures in the USA are similar: 95% of 12-17 year olds have internet access, with 74% having mobile access (via phone, tablet, etc.; including 71% of 12-13 year olds and 76% of 14-17 year olds). Significantly, 25% now access the internet mostly on their mobile phone (Pew, 2013). Among younger children, 31% of 9-10 year olds, and 69% of 11-14 year olds had a mobile phone in 2009 (Rideout, Foehr, & Roberts, 2010). EU Kids Online’s 2010 survey of 25 European countries found that, among internet-using 9-16 year olds, 87% go online at home, 49% of them in their bedroom and 33% via a mobile phone or other handheld device (Livingstone, Haddon, Gőrzig, & Ólafsson, 2011a).

Beyond access, researchers are tracking trends in use, including time spent and the social contexts and nature of use. However, such measurement is becoming more difficult as media and communication technologies are used simultaneously, often in the background of other activities, and across any location. Being ‘always on’ (Baron, 2008), in ‘constant contact’ (Clark, 2005) with their peers, has become routine, even taken for granted among children and young people. As a result, public concern about compulsive or excessive internet use or internet addiction is growing. ‘Problematic internet use’ is characterized by a cognitive preoccupation with the internet, an inability to control its use, going online to relieve emotional distress, and continued use despite negative consequences (Caplan, 2010; Gámez-Guadix, Villa-George, & Calvete, 2012; Van Den Eijnden, Meerkerk, Vermulst, Spijkerman, & Engels, 2008). Leung and Lee (2012) and Šmahel and Blinka (2012) found that excessive or problematic use is associated with a range of internet-related risks – harassment, invasion of privacy, and exposure to pornographic and violent content.

**Locating research on the risks of mobile and internet use**

Given the multidimensional nature of the problem, understanding the risks of mobile and internet use has attracted the attention of researchers from diverse disciplines. While the result is, helpfully, a highly multidisciplinary and multi-method field, it is also challenging that no single theoretical framework or standard methodology exists to unify the research enterprise and many definitional, measurement and interpretative challenges remain.

In this review, we have searched bibliographic databases and online sources across the disciplines of psychology, sociology, education, media studies and computing sciences, among others, using the keywords attached to this article. Both the technologies and the social practices of use are co-evolving rapidly, with new convergent, portable online devices reaching the overall market each year, as well as specific new trends in young people’s information and communication practices. The speed with which the evidence base becomes
out of date is therefore problematic. Consequently, our review concentrates on empirical research published in English since 2008. We further limited the field to research concerning children and adolescents (under 18 years old), though it is worth noting that, to the best of our knowledge, a review of research on the risk of harm to adults from mobile and online technologies remains to be written. Last, we have prioritised research on aggressive and sexual risks for two reasons. First, these are high on the agenda of policy, public and practitioner concerns, so an assessment of the evidence base, bringing together these usually-separate literatures is greatly needed. Second, most research has focused on these risks, allowing confidence in the identification of wider research strengths and gaps. Within these specifications, we are confident that the material reviewed here is representative of the field although, for reasons of space, it is not completely comprehensive.

The quality of empirical research in this field produced some difficulties for this review. In addition to the host of definitional and methodological challenges that bedevil this relatively new field of research, much policy making and practical intervention relies on quickly produced survey reports, too few of which undergo peer review for journal publication, some of which even omit to note the year of data collection (see Smith, 2010) or provide adequate details of sampling or analysis; for this reason, the EU Kids Online network has developed methodological guidance for the field (see the project home page, under supporting information links). For the present review, we have prioritised findings that meet high standards of evidence, such as those as required for publication in reputable peer-reviewed journals.

**Understanding the risks of mobile and internet use**

To systematise the array of risks on which research is now being conducted, the EU Kids Online network classified online risks to children as broadly focused on aggressive, sexual, value-related (e.g. visiting extremist sites) or commercial dimensions, although overlaps between these exist. They can be subdivided into *content risks* (which generally position the child as the recipient of mass produced content), *contact risks* (generally an adult-initiated online interaction which requires the child to participate, possibly unwittingly or unwillingly) and *conduct risks* (where the child is an actor or interactor within a wider peer-to-peer or networked interaction).

While many claims are made regarding value-oriented and commercial risks, little is known of whether and how they affect children; most publications address legal or policy issues, or focus on adults. Some exceptions are Mitchell and Ybarra (2007) on self-harm,
Bond (2012) and Bardone-Cone and Cass (2007) on pro-anorexia sites, Alao, Soderberg, Pohl and Alao (2006) and Biddle, Donovan, Hawton, Kapur and Gunnell (2008) on suicide sites, and Nairn, Fielder, Gardner, and Pitt (2007) and Sora and Yi (2010) on commercial messaging. More surprising, given the history of concerns regarding violence on television and in video games and film, little research has examined violent content in relation to the internet, although two large-scale surveys indicate that children themselves are worried by this in the UK (Safer Internet Centre, 2013) and Europe generally (Livingstone, Kirwil, Ponte, & Staksrud, 2013).

To date, research on aggressive and sexual risks has been addressed separately. The study of cyberbullying is largely anchored in the literature on traditional bullying (Olweus, 2012a, Smith, 2012, in press). The study of children’s access to online pornography (to be distinguished from the adult trade in illegal child abuse images) is approached from the tradition of research on children’s exposure to sexual content in mass media (Flood, 2007; Peter & Valkenburg, 2007). Research on online ‘grooming’ (the process by which adults approach children online or by mobile for the purposes of sexual abuse) is undertaken by child protection specialists (Martellozzo, 2011; Seto, Wood, Babchishin, and Flynn, 2012; Webster et al., 2012).

It is, on the one hand, a strength that the study of mobile and online risks is informed by the more established study of (offline) harms experienced by children. On the other hand, the diversity of academic traditions now combining their efforts in the study of internet and mobile risks compounds the present conceptual, definitional and methodological challenges facing this field. Consequently, this review situates evidence on both sexual and aggressive risks within the broader framework of adolescence, risk and resilience (Breakwell, 2009; Bynner, 2001; Coleman & Hagell, 2007; Schoon, 2006). This helps in identifying the risk and protective factors that can account for youthful experiences across risk types as well as suggesting beneficial interventions.

Some of these factors relate to the circumstances of children’s lives, but others relate to the nature of the technologies or contents that they engage with. Since not every encounter with an online risk is inevitably harmful, it is helpful to conceptualise online risks as affording harm, harm being a probabilistic outcome which depends on a host of contingencies that are reviewed in what follows. The same may be said for online opportunities, as these too afford but do not determine positive benefits for children; while consideration of such undoubted opportunities is beyond our present remit, see Hobbs (2010), Ito et al. (2013), OECD (2012) and Östman (2012).
The definition, nature and prevalence of mobile and online risk

Aggressive risks: cyber-aggression and cyberbullying

There are many types of ‘electronic’ or cyber-aggression, including flaming, online harassment, cyberstalking, denigration (put-downs), masquerade, outing, exclusion, putting up false profiles and distributing personal material against someone’s wishes (Pyzalski, 2012; see also Calvete et al., 2010). An analysis of abusive text messages and e-mails by Rivers and Noret (2010) found them to contain threats of physical violence, abusive or hate-related, name calling (including homophobia), death threats, ending of platonic relationship(s), sexual acts, demands/instructions, threats to damage existing relationships, threats to home/family, and menacing chain messages. The victim may be known to the perpetrator offline (e.g. from school, or former girlfriends/boyfriends), may come from certain groups (e.g. fans of a certain pop group or football team), but may also include celebrities, vulnerable people, school staff or victims known only from the internet (Pyzalski, 2012).

Some researchers have used general terms such as ‘cyber victimization’ (Law, Shapka, & Olson, 2010) or ‘online harassment’ (Hinduja & Patchin, 2010), while Vandebosch and van Cleemput (2009) used the term POP (potentially offensive internet and mobile phone practices). However, much research has used the term cyberbullying. Following Olweus’ definition of traditional bullying, one common definition of cyberbullying is: “An aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself” (Smith et al., 2008:376; Smith, del Barrio & Tokunaga, 2013). In addition to the important criterion of intent to cause harm, Olweus’ definition emphasises the imbalance of power and repetition, to discriminate bullying from other forms of aggression.

Other uses of the term cyberbullying emphasise repetition over imbalance of power (e.g. “when someone repeatedly harasses, mistreats, or makes fun of another person online or using cell phones or other electronic devices”; Patchin & Hinduja, 2012:15), imbalance of power over repetition (e.g. Wang, Iannotti, & Nansel, 2009), or they include neither criterion, as in: “intentional behaviour aimed at harming another person or persons through computers, cell phones, and other electronic devices, and perceived as aversive by the victim” (Schoffstall & Cohen, 2011:588). A six country study by Menesini et al. (2012) found that 11-17 year olds themselves gave most weight to imbalance of power in judging whether a scenario was a case of cyberbullying (except in France, where the term cyberviolence is used), followed by intentionality, and anonymity as a substitute for imbalance of power;
repetition or the public/private nature of the context were less important.

Repetition and intentionality become linked when a cyberbullying act ‘snowballs’ out of the perpetrator’s control. Slonje et al. (2012) found that, having seen information intended to cyberbully someone else, 9% of pupils forwarded the material to other friends, and 6% showed or forwarded it to the victim to bully him/her further. Thus a single act by one perpetrator may be repeated by others and thus experienced many times by the victim.

The importance of power imbalance is contested in the online and mobile domain, since neither physical strength nor strength in numbers is needed for cyberbullying. Vandebosch and Van Cleemput (2008) argued that a greater knowledge of ICT can create a power imbalance, having found that pupils with more advanced internet skills were more likely to have experience with deviant internet and mobile phone activities (such as impersonating someone else on a website, or bullying in virtual worlds). They also argued that anonymity can contribute to a power imbalance, since if the victim does not know the identity of the person bullying him or her, it is more difficult to respond effectively (Raskauskas, 2010; Slonje & Smith, 2008; Smith et al., 2008). However, if a victim does know the perpetrator, it usually being someone from the same school or vicinity (Smith et al., 2008) then conventional criteria of physical/psychological strength and peer group popularity may come into play (i.e., a victim may fear retaliating against a popular and stronger pupil who can take further revenge offline).

At present, opinion remains divided as to whether cyberbullying can be considered in a similar way to traditional bullying (Olweus, 2012a; Smith, del Barrio & Tokunaga, 2013), or whether linking it to other forms of cyber aggression is more useful (Bauman, Underwood & Card, 2013). What is clear is that the term cyberbullying is sometimes used too loosely, without reference to either repetition or power imbalance; for this reason, measurement procedures should be clearly specified.

In fact, not only are the key criteria contested but so is the measurement of cyberbullying. Berne et al.’s (2013) systematic review of 43 instruments found that few reported their reliability or validity. Some studies treat cyberbullying as a single construct (e.g. Study 1 in Law, Shapka, Hymel, Olson & Waterhouse, 2012), while others distinguish types according to the technology or platform used – for example, distinguishing internet from mobile phone bullying (e.g. Ortega, Elipe, Mora-Merchan, Calmaestra & Vega, 2009), although with the advent of smart phones, this is no longer straightforward. Indeed, the tools for cyberbullying are diversifying. Rivers and Noret’s (2010) survey in 2002 examined text message and e-mail bullying; but a few years later, Smith et al. (2008) examined bullying by
mobile phone calls, text messages, picture/video clip bullying, e-mails, chatrooms, instant messaging, and websites. Cyberbullying in online games (Tippett & Kwak, 2012) and virtual worlds (Coyne, Chesney, Logan, & Madden, 2009) is also now recognised.

Given differences in definition and measurement, it is not surprising that estimates of the prevalence of cyberbullying vary. The 25-country EU Kids Online survey of 9-16 year olds in 2010 defined bullying as a hurtful or nasty way of acting towards them face-to-face, by mobile phone calls or texts, or on the internet, that can often be quite a few times on different days over a period of time (Livingstone, Haddon, Görzig & Ólafsson, 2011a). Prevalence varied across countries, with 6% reporting being bullied online, 3% by using mobile phone or text, and 13% face-to-face. Figures for bullying others were lower – at 3%, 2% and 10% respectively. Using a definition that also includes power imbalance, Olweus’s (2012a) surveys between 2007 and 2010 nonetheless found similar percentages in the US (at around 4-5%, for 8-19 year olds) and Norway (at around 3-4%, for 9-17 year olds). Also emphasising repetition, Genta et al. (2012) surveyed 12 to 15-year olds in Italy, Spain, and England in 2008, finding that the prevalence of repeated bullying (whether as bullies or victims) ranged from 1% to 3%, depending on country and type of bullying. Similar findings were obtained by Salmivalli and Pöyhönen (2012) in Finland in 2007/8 and by RSM McClure Watters (2011) in Northern Ireland in 2011.

Some researchers find these low figures difficult to believe. In commenting on Olweus (2012a), Hinduja and Patchin (2012a: 541) stated that “Olweus’ findings that 4.1-5.0% of youth have been cyberbullied and 2.5-3.2% of youth have cyberbullied others are simply out of line with the weight of the available evidence”. Their own studies suggest 20% of 11 to 18 year olds have been a victim of cyberbullying (Hinduja & Patchin, 2012b), and in a review of 35 published articles, they found on average 24% of pupils had been cyberbullied and 17% had cyberbullied others. As another example, a Turkish survey of 8-11 year olds reported that 18% had (ever) cyberbullied others, and 27% had (ever) been cyberbullied (Arslan, Savaser, Hallett & Balci, 2012), while Marsh, McGee, Nada-Raja and Williams (2009) found that 8% of 15 year old boys and 14% of girls in New Zealand had received nasty text messages at school several times that year. Using their broader POP definition, Vandebosch and van Cleemput (2009) found 62% victims and 53% perpetrators at least once over the past 3 months.

Olweus (2012b) responded by emphasising the importance of the time reference period (in the past month, or year, or ‘ever’) and frequency criteria (just once, monthly, more often, etc.). As an example of this, O’Moore and Minton (2009) gave an Olweus-type questionnaire
to 12 to 16 year old in the Republic of Ireland, finding that frequencies of cyberbullying
others and being cyberbullied were 8.7% and 14.2% for those to whom it only happened once
or twice, but dropped to 1.6% and 2.8% respectively if the standard ‘2 or 3 times a month’
criterion was used (similar differences are noted in Livingstone, Haddon, Görzig & Ólafsson,
2011a).

In sum, a range of factors can be identified that affect prevalence estimates of
cyberbullying or cyber aggression, including frequency, time reference period, definitions
that do or do not include repetition and/or imbalance of power, as well as the nature and age
of the sample, the emphasis on particular media or bullying practices, and the date of survey
administration, which is important at a time of social and technological change. In terms of
incidence, it seems that occasional or one-off occurrences may be reported by over 20% of
young people but serious or recent or repeated incidents are reported by only around 5%, less
than for traditional bullying.

Sexual risks: pornography, stranger danger, sexting
As with aggressive risks, estimates of the prevalence of sexual risks vary according to the
definitions employed. The term ‘pornography’, for instance, can refer to diverse kinds of
sexual content ranging from ‘top shelf’ or partial nudity to graphic depictions of sexual
intercourse to violent or illegal images of abuse. The ethical difficulty of asking children
exactly what they have seen without introducing them to unfamiliar sexual ideas compounds
the challenge of identifying exactly what they have been exposed to.

The question of intentionality further confuses, since it is widely accepted that
adolescents may deliberately seek pornography but, equally, social desirability concerns
make unlikely that they will fully disclose this. Moreover, the internet ‘pushes’ pornography
at those seeking informational or health or other material, resulting in accidental exposure
(via pop-ups or misleadingly-named sites). Jones, Mitchell and Finkelhor (2012:181)
surveyed US 10-17 year olds in 2010 and found that between 15% (10-12 year olds) and 28%
(16-17 year olds) had been “exposed to pictures of naked people or people having sex
without seeking or expecting such pictures” in the last year. The EU Kids Online project
asked 9-16 year olds if, in the past year, they had seen “pictures, photos, videos [which were]
obviously sexual – for example, showing people naked or people having sex” (Livingstone,
Haddon, Görzig, & Ólafsson, 2011b). This found similar results to the US findings: 14% had
seen sexual images online, with older teenagers four times more likely than the youngest to
have seen such images.
Defining exposure instead in terms of intention, Peter and Valkenburg (2009:416) asked Dutch adolescents how often “they had intentionally looked at” images or movies with exposed genitals or in which “people are having sex” in the previous six months. Based on a sample whose average age was around 17 years, they found that only 9% said they had never encountered such material (although their later survey found that most - 75% - had not seen visible genitals online in the past six months; Peter and Valkenburg, 2011a). Also assuming intentional exposure, Brown and L’Engle (2009:138) asked US 12-14 year olds how often, in the past year, “did you see X-rated movies?”, how often they “read magazines like Playboy, Playgirl, Penthouse, or Hustler?” and “How often do you view pictures of naked women or men on your computer or the internet?”; the percentage who had done any of these ranged from 21% (12 year old girls) to 66% (14 year old boys).

While traditional conceptions of pornography refer to professionally-produced, mass distributed images, online and mobile technologies make it ever easier for young people to create and circulate sexual images themselves. ‘Sexting’ is the most recent mobile and online risk to gain public and research attention. A range of definitions is in use, from adolescents’ own account of ‘sexting’ as the willing exchange of messages between romantic partners (Lenhart, 2009) to definitions that regard it as the digital extension of the long-established coercion of girls by boys to provide sexual services or to conform to particular sexual expectations (Albury, 2013; Ringrose et al., 2012; Ševčíková, Simon, Daneback, & Knapilík, 2012). As with pornography, teenagers and adults may not agree on where to draw the line between acceptable sexual exploration between peers and inappropriate or abusive messaging. The illegality of sexually explicit images of minors and the consequent intervention by law enforcement has exacerbated the tensions surrounding this phenomenon (Arcabascio, 2010; Salter, Crofts & Lee, 2013).

Definitional diversity has led to wide variation in estimates of prevalence, ranging from 7% (Mitchell, Finkelhor, Jones, & Wolak, 2012) to 15% (Lenhart, 2009; Rice et al., 2012; Livingstone et al., 2011b) to as many as 48% (National Campaign to Support Teen and Unplanned Pregnancy, 2008). Lounsbury, Mitchell, and Finkelhor (2011) argue for definitional clarity regarding technology (mobile or internet), messaging (images or written exchanges), and participants (under or over 18 years; communicating with known peers or unknown contacts). Their aim is to distinguish potentially criminal from legal activity; it seems also important to distinguish harmful from harmless activity (as they do in a related paper; Wolak & Finkelhor, 2011).
While pornography and ‘sexting’ occasion considerable public concern, so-called ‘stranger danger’ has aroused the greatest anxiety, and news about paedophiles seem rarely out of the headlines (Staksrud, 2013). In relation to online sexual solicitation (whether from strangers or from those known to the child), Jones, Mitchell, and Finkelhor (2012:180) asked US 10-17 year olds in 2010, “In the past year, did anyone on the internet ask you for sexual information about yourself when you did not want to answer such questions? I mean very personal questions, like what your body looks like or sexual things you have done?,” “In the past year, did anyone on the internet ever try to get you to talk online about sex when you did not want to?,” and “In the past year, did anyone on the internet ever ask you to do something sexual that you did not want to do?”. They found the prevalence of online sexual solicitation to vary from 2% among 10-12 year olds rising to 14% among 16-17 year olds (with an average of 9% across the age range).

It is difficult to relate such findings to offline sexual abuse. While reliable figures are hard to come by, the UK’s National Society for the Prevention of Cruelty to Children estimated that 5% of UK children suffer contact sexual abuse at some point during childhood, with some 10,000 new victims each year (Harker et al., 2013). The Child Exploitation and Online Protection Centre (2013) receives reports from around 1,000 children each year concerning online victimisation by adults, so this suggests that abuse by perpetrators known to the child offline is far more common than grooming by strangers online, although doubtless much goes unreported. Research is now tracing the processes by which offline and online contacts can become intertwined in the actions of both perpetrators and victims (Webster et al., 2012). However, as Jones et al (2012) found in their 2010 US survey, the majority of unwanted online sexual solicitations are not pursued offline– 3% of 10-17 year olds reported “aggressive solicitations” online in which “offline contact was attempted or made”(p.182).

While many unwanted sexual encounters, online or offline, are perpetrated by known adults, public anxiety remains focused on ‘strangers.’ This, in itself, is difficult to determine online since children make many contacts online with people they have not met face to face. The EU Kids Online survey found that 30% of European 9-16 year olds had made contact online in the previous year with someone they did not already know (ranging from 13% of 9-10 year olds to 46% of 15-16 year olds); in all, 9% had gone to a meeting face-to-face with someone that they first met on the internet (again, more teenagers than younger children) (Livingstone et al., 2011a). On one description, then, ‘meeting strangers’ is common, though face-to-face meetings with such contacts are rarer, and most of those are within the friendship
circle (i.e. with ‘friends of friends’). Notions of friend and stranger are, it seems, newly in flux because of the ease with which online contacts can be made, challenging safety interventions and policy frameworks as well as the definitions and measures employed by researchers.

**Comparing findings across individuals, culture and time**

*Age and gender differences*

Reviewing cyberbullying, Tokunaga (2010) argued that there is a curvilinear relationship with age, with a peak around 13-15 years. In the Czech Republic, Ševčíková and Šmahel (2009) also found 12-15 year olds most involved as cyber aggressors, although the proportion of cyber victims was higher at 16-26 years, and both roles were present across the lifespan. In the US, Beran, Rinaldi, Bickham and Rich (2012) found incidence to approximately halve between high school and college, but with some continuity of involvement. For sexual risks, the incidence of exposure to pornography, sexual messaging or stranger contact is generally found to increase over adolescence (Livingstone, et al., 2011b), but with higher risks for teenagers than adults (e.g. Baumgartner, Valkenburg & Peter, 2010b).

The area of gender differences in cyberbullying has been described as “fraught with inconsistent findings” (Tokunaga, 2010:280). Some find boys more involved than girls (e.g., Calvete et al., 2010), some find girls more involved than boys (e.g., Rivers & Noret, 2010), and some find few or no significant differences (e.g., Smith et al., 2008; Livingstone et al., 2011b). Insofar as an overall picture can be discerned, it seems that while boys are more engaged in traditional bullying than girls, girls can be as much or even more engaged in cyberbullying, possibly because cyberbullying is more verbal or relational rather than physical, and is now often located on social networking sites (Görzig, 2011; Smith, 2012; Beckman, Hagquist & Hellström, 2013).

Regarding sexual risks, Livingstone, Kalmus and Talves (in press) concluded that boys were a little more likely than girls to have seen sexual images online and to receive sexual messages. This may reflect cultural norms that tend to sanction boys’ engagement with pornography more than girls’, or it may be because boys engage in more risky online activities such as having a public social networking profile or making new online contacts. On the other hand, a content analysis of personal information posted on social networking sites found that girls included more risky and sexual content than boys (Pujazon-Zazik, Manasse, & Orrell-Valente, 2012). As Baumgartner, Valkenburg, and Peter (2010b) add from their survey findings, adolescent girls are more at risk of sexual solicitation online than are
boys, but most are highly aware of this risk and do not seek it out or see it as beneficial.

**Cross-national comparisons**

To understand cross-national differences, the EU Kids Online study clustered European countries in terms of measured levels of children’s internet use, online opportunities and risks experienced, and preferences for particular strategies of parental mediation of the internet. This resulted in a four-fold classification: ‘supported risky explorers’ (Denmark, Finland, the Netherlands, Norway and Sweden); ‘semi-supported risky gamers’ (Bulgaria, Cyprus, Czech Republic, Estonia, Poland and Romania); ‘unprotected networkers’ (Austria, Hungary, Lithuania and Slovenia); and those ‘protected by restrictions’ (Belgium, France, Germany, Greece, Ireland, Italy, Portugal, Spain, Turkey and the UK) (Helsper, Kalmus, Hasebrink, Sagvari, & De Haan, 2013).

How can these and other differences be explained? Levels of socio-economic stratification, regulatory framework (more or less stringent), technological infrastructure (more or less developed) and educational system (number of years, inclusion of educational technology) have all been found to shape children’s online risks (Livingstone, Haddon, Görzig, & Ólafsson, 2011a). However, the differences among individuals are generally considerable larger than the differences among countries, at least within Europe (Genta et al., 2012; Livingstone, Haddon, & Görzig, 2012; Vazsonyi, Machackova, Ševčíková, Šmahel, & Cerna, 2012). Looking beyond Europe, initial indications of cultural factors are emerging (Child Exploitation and Online Protection Centre, n.d.; Davidson & Martellozzo, 2010; Family Online Safety Institute, 2011; Gasser, Maclay, Palfrey, & et al., 2010), but no strong predictive framework for how culture affects the consequences of mobile and online risk has yet been formulated or tested.

**Trends over time**

As use of online and mobile technologies has become more widespread, a common perception is that both risks and harms are increasing (Sabella, Patchin & Hinduja, 2013). Is this a matter of increased public awareness, whether fanned by the media or because children are spending more time online? Or does the evidence reveal a genuine rise in risk or harm or both?

The three waves of the nationally representative Youth Internet Safety Survey, conducted among US 10-17 year olds in 2000, 2005 and 2010 suggests that the prevalence of online sexual risks depends on the affordances of the online environment and the degree of policy effort to improve safety (for waves 1 and 2, see Wolak, Mitchell & Finkelhor, 2006; for wave 3, see Jones, Mitchell & Finkelhor, 2012). Unwanted sexual solicitations declined
over the three time points, from 19% to 13% to 9%; a change which they attribute in part to
the policy action to close or moderate the chatrooms initially so popular among adolescents
(and since largely replaced by social networking sites). Online harassment (which they
defined as feeling worried or threatened because someone was bothering or harassing you
online or using the internet to threaten or embarrass you by posting or sending messages
about you for other people to see) increased from 6% to 9% and then 11%, this being more
marked for girls; they suggest this increase could reflect the increase in internet use over the
period. Unwanted exposure to pornography first increased from 25% to 34%, but then
decreased to 23% by 2010; this may reflect behind-the-scenes industry effort to control pop-
ups and spam, much of which was pornographic.

In relation to cyberbullying, Rivers and Noret (2010) found that prevalence, measured
by annual surveys of 11-13 year olds in a northern British city, increased from 2002 to 2004
but then levelled off by 2006. Updating this picture, Tippett and Smith (submitted) surveyed
four secondary schools in England in 2008 and 2011, finding a decrease in traditional
bullying (both as perpetrators and victims) but not in cyberbullying by mobile and internet.
Moreover, by 2011 more of the cyberbullying was on social networking sites (for 69% of
victims, compared to 42% in 2008). In the US, Olweus (2012a) found a slight upward trend
in cyberbullying from 2007 to 2010 (but a slight downward trend in Norway). Ybarra,
Mitchell and Korchmaros’s (2011) Growing Up with Media survey of 10-15 year olds in
2006, 2007 and 2008 found that “most rates of youth violent experiences online were stable
over the 36-month observation period” (p.1379), although there was some increase in
perpetration of harassment online.

Bringing research on different risks together, in their longitudinal survey of 10,000
Flemish primary school children (averaging 11 years), Valcke, De Wever, Van Keer, and
Schellens (2011) calculated an Unsafe Internet Usage Index to capture a range of risk
experiences. This revealed a very small increase from 2005 to 2008 but then no change to
2009. However, within this broad picture, particular risks rose and fell on an annual basis.
This could reflect variation in children’s risky behaviour (which increases with digital skills),
the affordances of the internet (or, specific sites and services popular at any one time) and the
kinds of parental safety guidance received (which have also increased over time).

In summary, while much remains to be researched in this regard, it is striking that,
over the period when access to online and mobile technologies increased dramatically, there
was no equivalent evidence of a clear of substantial increase in either risk or harm to
children. One possibility is that the internet affords no greatly increased risks to children, than
they would have encountered offline. Another is that there is an associated risk of harm, but this has been offset by increased awareness raising efforts and industry controls. Yet further possibilities may be identified in future research.

**The harm associated with mobile and online risk**

Thus far, we have reviewed the evidence regarding children’s exposure to risks online. But as stated at the outset, this is distinct from the question of harm. However, there are few equivalents online of the accident or crime statistics to be found regarding danger to children offline (for instance, on the roads - a commonly drawn parallel with risk of harm in cyberspace; Byron, 2008). In other words, it is not really known how many children have been harmed as a result of an online experience; those concerned with sexual crimes against children, for example, consider that their statistics greatly underestimate the underlying levels of harm linked to internet or mobile activities (for the UK, see Child Exploitation and Online Protection Centre, 2013; for the US, see Wolak, Finkelhor, & Mitchell, 2012). To assess whether children are harmed by pornography or cyberbullying, researchers generally rely on subjective self-report measures, and few have conducted longitudinal studies that can track the later consequences of exposure to risk. Nonetheless, the growing evidence base now points to some evidence for harm, although how this might be compared to the other harms experienced by children requires further research.

**Aggressive risks and harm**

Victims of cyberbullying express a variety of emotions: anger, sadness, frustration, embarrassment, stressed, fright, loneliness and depression (Didden et al., 2009; Ortega et al., 2009), although this is not inevitable. Ortega et al. (2012) found that 22% of mobile victims and 32% of internet victims reported being not bothered, especially boys and those victimised less often. Cyber victimization is associated with a range of psychosocial problems, including affective disorders (Topcu, Erdur-Baker, & Capa-Aydin, 2008), depression (Estévez, Villardón, Calvete, et al. 2010; Perren, Dooley, Shaw, et al. 2010; Wang, Nansel, Iannotti, 2011; Olenik-Shemesh, Heiman, & Eden, 2012); and behavioural problems including substance use (Hinduja & Patchin, 2008); however a large number of cross-sectional studies in this area have not established cause-and-effect.

A few studies have assessed longitudinal relationships. Schultze-Krumbholz, Jäkel, Schultze and Scheitauer (2012) found that cyberbullying victimization predicted depressive symptoms 3-6 months later in girls but not boys. Over a six month period, both Machmutow, Perren, Sticca and Alsaker (2012) and Gámez-Guadix, Orue, Smith and Calvete (2013) found
that cyber victimization predicted increased depression in both boys and girls, and also problematic internet use in the latter study. Gámez-Guadix et al. (2013) also found that higher depressive symptoms and more substance use predicted later cyber victimization, suggesting a vicious cycle unfolds for victims over time. Over a longer time frame, Lester, Cross, and Shaw (2012) found that levels of traditional victimisation and perpetration at the beginning of secondary school predicted levels of engagement in problem behaviours two years later; but although cyberbullying predicted problem behaviours, it was not an independent risk factor over and above traditional victimisation and perpetration.

Because offline bullying often involves physical intimidation or pain, it might be assumed that the severity of harm is greater than for cyberbullying; on the other hand, the affordances of online and mobile communication (such as anonymity, wide audience, difficulty of escaping) might make cyberbullying more harmful. Campbell, Spears, Slee, Butler and Kift (2012) did find a greater negative impact of being a cyber victim, but most research shows little difference. Hinduja and Patchin (2010) found that being a victim of cyberbullying was associated with suicidal thoughts but no more than is reported by victims of traditional bullying; as did Hay and Meldrum (2010), and Bauman, Toomey and Walker (2013; though with some gender interactions). Gradinger, Strohmeier, and Spiel (2009) found that being a cyber-victim was associated with similar degrees of depressive and somatic symptoms as for traditional victims; and Beckman, Hagquist and Hellström (2012) found this for both victims and perpetrators.

Olweus (2012a:534) tentatively concluded that “if the student is exposed to both traditional and cyber bullying, the additional impact of cyber bullying seems to be negligible”. Yet most studies find that those children who experience both types of bullying report worse symptoms (Brighi et al., 2012; Campbell et al., 2012) and some also find the consequences worse if children are involved as both cyber victims and cyber perpetrators (Beckman, Hagquist & Hellström, 2012; Gradinger et al., 2009), although not all agree (Campbell et al., 2012; Estévez et al., 2010).

A well-established finding is substantial overlap between victimisation and perpetration online and offline. For example Mishna, Khoury-Kassabri, Gadella and Daciuk (2012) found 45% of those involved to be cyber bully-victims. Based on path analysis (of cross-sectional data), Kowalski, Morgan and Limber (2012: 516) suggested that “we would expect very frequent perpetrators of traditional bullying to also begin bullying electronically and to become victims of cyberbullying themselves as their frequency of electronic perpetration increases.” Longitudinal studies are urgently needed to test such models further.
Sexual risks and harm

In relation to sexual risks, research often stops at measuring children’s exposure, apparently assuming that exposure to pornography or ‘sexting’ is inevitably harmful (or that children cannot report on any harm that results). In the US, Jones et al. (2012:181) asked 10-17 year olds who had seen pornography if they were “very or extremely upset”; in their 2010 survey, nearly half the 10-12 year olds but only a fifth of the 16-17 year olds described the experience in this way. Of the 14% of 9-16 year olds who had seen online pornography in the EU Kids Online project, around one third said that they had been bothered or upset by this. For sexting, among 15% of 11-16 year olds who had seen or received a sexual message online, a quarter reported being bothered by this. While these risks were more often encountered by older teenagers, a higher proportion of girls and younger children found them upsetting (Livingstone, et al., 2011b; see also Baumgartner, Valkenburg & Peter, 2010b; Ringrose et al., 2012).

Finding that only a minority of children who experience sexual risks are upset by them questions those policy interventions designed to prevent harm by preventing exposure. If children’s self-reports are to be relied upon, one might conclude that some efforts to prevent risk are too restrictive, especially if they also prevent teenagers’ search for sexual information or their expression of sexual identity and interest. An alternative view holds that children cannot know the harmful effects of such exposure, especially in the long term. Owens, Behun, Manning and Reid’s (2012: 116) review of the effects of exposure to pornography finds tentative evidence that “youth who consume pornography may develop unrealistic sexual values and beliefs.” For example, Peter and Valkenburg (2009) found that increased exposure to online pornography led to a stronger belief in women being sex objects (although the reverse effect was also supported), suggesting that policy makers should work to minimise such risks.

Even for online sexual solicitations, the Youth Internet Safety Survey found that only a few of the US 10-17 year olds (more often younger children) said that these were distressing (Jones et al., 2012). The EU Kids Online survey found that, among the 9% of 9-16 year olds who had met an online contact offline, one in nine of these (or 1% of all respondents) reported being bothered in some way by what happened. Yet for this small minority, painful and even tragic experiences can result, as analysis of cases reported to the UK children’s helpline reveals (ChildLine, 2012). Determining which online contacts pose a threat is a difficult decision for a child or parent to make, especially given the complex
technical and social tactics employed by sexual offenders (Quale & Taylor, 2011; Webster et al., 2012).

**Factors that increase risk of harm or protect against them**

Which risk and protective factors explain why some children are more likely to encounter risk online, or to find it harmful, compared with other children? No dominant model has yet emerged in this still-new field of online risk, but researchers are now drawing on established literatures on (offline) risk and risk-taking in adolescence.

In terms of **risk-taking**, those who take risks in one domain are likely to take them in others also (Jessor, 1991; Carson, Pickett, & Janssen, 2011; Guilamo-Ramos, Litardo, & Jaccard, 2005). In relation to adolescents, one explanation put forward is that teenagers combine sensation-seeking with a relative lack in impulse control (Steinberg et al., 2008; Van Nieuwenhuijzen, et al., 2009). This could account for the associations between online and offline risks, especially since mobile and online communication is often anonymous or asynchronous, thereby facilitating disinhibition (Suler, 2004). Evidence linking offline and online risk can be found in the finding that involvement in traditional bullying predicts cyberbullying (see above), or that those who engage in more risky offline (and risky online) activities are more likely to be involved in sexting (Livingstone & Görzig, 2012).

In the established literature on **childhood vulnerability** also, it has long been known that risk factors tend to compound each other (Schoon, 2006; 2007). The resulting vicious circle increasingly appears to encompass online risk (Munro, 2011; Wells & Mitchell, 2008). For example, Bobkowski, Brown, and Neffa (2012) report that, for girls who reach puberty earlier than their peers, the internet may provide a route to sexual expression and exploration, this placing them further at risk. Slater, Henry, Swaim and Cardador (2004) found that the effect of violent media on aggression is greater among children who are alienated from school, who are more sensation seeking, or who feel victimised by peers. Wolak, Finkelhor, Mitchell and Ybarra (2010) report that those vulnerable to grooming tend to be high risk youth with a history of prior sexual abuse – rather than the lonely children of media panics. Some researchers seek a single underlying personality or behavioural factor to account for the range of risks that children encounter (Donovan & Jessor, 1985; Jessor, 1991); if this were identified, it could account for both online and offline risks and so aid the development of prevention strategies for online risks (Brady & Donenberg, 2006; Hale & Viner, 2012; Jackson, Henderson, Frank, & Haw, 2012).
Particular attention has long been paid to risk factors at the levels of individual personality, family and peer relations and the wider environment (Breakwell, 2009), and each of these is now being examined in relation to online risk. In terms of personality, it seems that sensation seekers and those facing psychological difficulties take more risks offline and online and, as a result, are more likely to receive sexual messages online (Livingstone & Görzig, 2012); sensation seekers are also more likely to use online pornography (Peter & Valkenburg, 2011a). In their longitudinal study of Dutch adolescents, Machmutow et al. (2012) found that for victims of cyberbullying, coping strategies rated as helpless were associated with more depression. Self-esteem also matters: Van den Heuvel, Van den Eijnden, Van Rooij, and Van de Mheen (2012) found that adolescents with low self-esteem were more likely to go to further meetings with online contacts, even after an initial meeting offline. Relatedly, use of pornography is linked to low self-esteem (Owens, Behun, Manning, & Reid, 2012). On the other hand, highly confident youth may also seek out online risks (Vandoninck, d’Haenens, & Donoso, 2010), suggesting that the role of self-esteem is complex. As regards other personality factors, empathic ability maybe a protective factor against involvement in cyberbullying (or its lack, a risk factor); such associations have been found to be stronger for affective empathy than cognitive empathy (Ang & Goh, 2010; Topcu & Erdur-Baker, 2012). Further, narcissistic exploitativeness and normative beliefs approving of aggression have been linked to cyberbullying (Ang, Tan & Mansor, 2011). Gini, Pozzoli and Hymel (2013) found from a meta-analysis that moral disengagement appeared an equally prominent feature of both traditional and cyber bullies.

There is evidence that parenting contributes to vulnerability to online and mobile risks much as it does to offline risks. Lack of parental involvement is associated with vulnerability to being groomed online for sexual abuse (Whittle, Hamilton-Giachritsis, Beech & Collings, 2013), and with involvement in all kinds of bullying, including cyberbullying (Wang et al., 2009). The nature of parental involvement can be further clarified: Law et al. (2010) linked adolescent online aggression to lack of communication with parents but not to parental efforts to regulate their children’s internet use (a finding replicated by Soo, Ainsaar & Kalmus, 2012).

Peer relations are important. Williford et al. (2013) showed that cyberbullying was in part a classroom-level phenomenon, in an analysis of KiVa data in Finland. Baumgartner, Valkenburg and Peter (2010a) found that perceived peer involvement and support was a determinant of adolescents’ risky online behaviour. Similarly, Rice, et al.’s (2012) survey of 14-17 year olds found that sexting was predicted by peers’ levels of sexual activity. However,
Peter and Valkenburg’s (2011a) longitudinal study of adolescents who seek out online pornography found no effect for relationship status or attachment to friends, suggesting that having friends is less important than whether they are perceived to support risky activities.

Less research has examined wider environmental factors, although vulnerability to online grooming is associated with poor living environment and low socio-economic status (Whittle, Hamilton-Giachritis, Beech & Collings, 2013). Looked at in terms of protective factors, Brooks, Magnusson, Spencer, and Morgan (2012) found that a strong sense of belonging to family, school or neighbourhood protects children from health risk behaviours (including sexual risks; see Willoughby et al., 2007), raising the possibility that these would be useful factors to include in future studies of online risks. Relatedly, Mitchell, Wolak, and Finkelhor (2007) found a drop in online sexual risks among white and affluent children between 2000 and 2005, suggesting that safety messaging was more effectively reaching advantaged children.

Bringing these factors together permits identification of different groups or trajectories of risk. In their four-wave longitudinal study of Dutch 12-18 year olds, Baumgartner, Sumter, Peter and Valkenburg (2012) distinguish (i) no-online-risk adolescents (70% of their sample) from the (ii) moderate-online-risk group (24%), whose generally low level of online risk rises in mid-adolescence, and the (iii) high-online-risk group (just 6%). Most of the first (no-online-risk) group also engaged in no offline risk. The two online risk groups were more likely to be sensation seekers and to have lower life satisfaction and/or family difficulties, supporting the above findings on risk factors. However, among the online risk groups, some reported no offline risk (and online-only risk was far more common than offline-only risk). This suggests that, among sensation seekers or those facing problems, the internet affords particular opportunities for adolescents to experiment with risky or transgressive behaviour. Whether or not these are greater than the opportunities available for risk-taking offline is unknown, however.

Some researchers have examined children’s relations with online and mobile technologies to identify further possible risk factors. The more the time children spend online, the more likely they are to be a cybervictim (Hinduja & Patchin, 2008b; Smith et al., 2008) or perpetrator (Mishna et al., 2012). Vandebosch and van Cleemput (2008) found that pupils with more advanced digital skills engaged in more ‘deviant’ online and mobile activities. Wolak, Finkelhor and Mitchell (2008) identified four online interaction styles among US adolescents. ‘High-risk unrestricted’ interactors received twice as many aggressive solicitations as ‘low-risk’, ‘friend-mediated’ or ‘cautious’ interactors. These high-
risk adolescents were older, used the internet more, reported more offline bullying or assault, and were higher on the Child Behavior Checklist for rule-breaking, depression and social problems.

The personality and behavioural risk facts discussed earlier influence the ways in which adolescents use the internet and this, in turn, affects the risks that result (Livingstone, Haddon & Görzig, 2012). However, the particular affordances of online and mobile technologies may interact with user characteristics. Mitchell, Wolak, and Finkelhor (2008) found that although young bloggers do not interact with strangers more often than non-bloggers, and nor are they at greater risk of sexual solicitation, they are at increased risk of online harassment; this may be because, in blogging, they have expressed in public some potentially controversial or personal views.

The challenge for research on affordances is that these are always changing as providers continue to innovate. For example, Ybarra and Mitchell (2008) found more unwanted sexual solicitations to come via chatrooms and instant messaging than social networking sites, doubtless because chatroom contact is often anonymous or disguised while instant messaging is private. Yet as social networking became more popular, research conducted just a few years later found that social network users encounter more risks than non-users, especially if their levels of digital skill are higher or if they engage in risky practices (such as having a public profile, displaying personal information or having a very large number of ‘friends’) (Staskrud et al., 2013). One might surmise that in the earlier study, the risk-taking adolescents sought out chatrooms as the most suitable location for high risk interactions with strangers, but once these were closed, and once it became possible to create large number of contacts on social networking sites, their practices – and thus the location of any risks experienced – altered.

**Conclusions and future directions**
The rapid adoption and use of online and mobile technologies by children is associated with some risk of sexual and aggressive harm. However, while estimates of prevalence depend on the nature of the risk, as well as on its definition and measurement, most risks are encountered by a small minority of adolescents, fewer than might be assumed from popular anxieties and mass media coverage (Vandebosch et al., 2013). Since the present climate in many developed countries favours evidence-based policy making, it is constructive that the past decade has seen an escalation in researchers from multiple disciplines combining forces to raise awareness, produce research evidence, and initiate multi-stakeholder efforts to
mitigate harm. There are vigorous debates and some signs of improvement concerning the clarity and rigour of research definitions, sampling and measures.

*Have risks increased?*

In terms of substantive conclusions, we note that the risks of cyberbullying, contact with strangers, sexual messaging (‘sexting’) and pornography generally affect fewer than one in five adolescents, albeit with significant variations depending on risk definitions, target age group and the affordances of widely-used technologies or services. Despite the rise in children and young people’s use mobile and online technologies, there is little compelling evidence that online risks are increasing commensurately. To those who find it implausible that new technologies have not increased the risk of harm in children’s lives, it is worth noting that, over the period when internet and mobile use have risen sharply, long term measures of harm to children reveal little or no increase over recent years (Madge & Barker, 2007; Maughan, Collishaw, Meltzer & Goodman, 2008), and some reductions in bullying and victimization (Finkelhor, 2013).

It remains possible that technology is displacing older forms of risk (for example, some perpetrators seeking to groom children for sexual abuse may now operate online in preference to offline approaches; or, when children seek pornography they now prefer to access it online rather than offline). It is also possible that technology has become so embedded in children’s communicative activities that when their experiences become aggressive or inappropriately sexual, online and mobile communication are increasingly likely to be implicated, along with (rather than instead of) face to face communication. It may also be that some risks are increased by the use of new technologies (for example, exposure to pornography or receipt of hostile messages may be amplified by the convenience or anonymity of activities conducted online) but that, partly as a result of such exposure, and partly because of the parallel increase in policy and practitioner efforts to raise awareness and improve safety measures, children are becoming more resilient and so better able to cope; this too could explain why measures of harm have not risen commensurately.

*Do risks result in harm?*

It is important to recognise that not all online risks result in harm, though since this is generally measured by self-reported upset or other adverse consequences, one cannot be conclusive on this point. Nonetheless, there is evidence of a range of adverse emotional and psychosocial consequences, and these are especially convincing when revealed by longitudinal designs that follow up with those affected several months after initial exposure to risk. By situating the study of online and mobile risk in the more-established tradition of
studying offline risk in children’s lives, researchers have begun to examine whether the risk and protective factors already identified play a role also in explaining online risk. Thus far, there is evidence that the following factors are important for risks of harm resulting: personality factors (sensation-seeking, low self-esteem, moral disengagement, psychological difficulties), social factors (lack of parental support, peer norms) and digital factors (online practices, digital skills, the affordances of specific online sites and services).

A general conclusion is that children who are already vulnerable offline are likely also to be vulnerable online. However, the variance explained by traditional risk factors is fairly low, suggesting that further factors are yet to be found to account for online vulnerability, and these may lie in either the offline or online context or the interaction between the two. The affordances of a changing array of popular online sites and services have particular implications for aggressive, sexual and other risks that have long been implicated in children’s lives. Thus research is turning to an exploration of the interaction between young people as users and their socio-technological environment. Peter and Valkenburg (2011b) hypothesise that the developmental tasks faced by adolescents dovetail with the specific affordances of the internet (for example, between the need to develop an identity and the opportunity to experiment with self-presentation on social networking sites, or between the need to develop intimate relations and the ease of self-disclosure online compared with face-to-face situations). This opens up possibilities for guiding adolescents, and younger children, in the specific use of social networking or chat sites, or for designing safety into sites in the light of knowledge regarding the practices and needs of young people.

**Implications for research and practice**

Despite the considerable body of research reviewed in this article, there remain significant challenges for both research and practice. In the coming years, the empirical research agenda regarding online risk should prioritise the need for (i) explicit assessment not only of risk but also of any harm associated with that risk, rather than simply presuming that harm results, (ii) longitudinal research designs to determine the developmental pathways of involvement, and whether harmful effects are long-lasting, (iii) studies of pre-adolescent children, who are now gaining internet and mobile access often via a personal device (smart phone, tablet or games machine) that their parents may not understand or be easily able to monitor, (iv) a systematic analysis of the key risk factors, and protective factors that can help children become more resilient to risk when they encounter it, therefore minimising harm, (v) evaluations of awareness raising and harm reduction interventions, few of which have yet been conducted, and (vi) exploratory research to identify new and emerging risks, including for particular
groups of children or under particular conditions as the social and technological landscape continues to innovate. Whether research satisfactorily captures children’s experiences of online and mobile risks is also contested, and one approach is to make more use of young people themselves as researchers (Spears & Kofoed, 2013).

Also challenging, conceptually and empirically, is the importance of gaining a more subtle yet systematic grasp of the shifting relations between online and offline risks. Often, risk is studied either online or offline, making it difficult to assess whether the advent of online and mobile technologies has extended the risk of harm to children or whether the proportion of children at risk is largely unchanged, with only the means by which it occurs changing. Some progress has been made especially in relation to (cyber)bullying, to ensure that online risks are examined in relation to the related offline risks. However, as children further integrate online and mobile technologies into their daily lives, distinguishing and comparing online and offline risk will become more difficult, demanding that researchers and practitioners recognise how a complex interplay among social norms and technological affordances shapes any particular communicative context. While recent research has progressed in terms of defining and measuring risk, the further embedding of online in offline contexts will increasingly challenge our research methodology.

**Policy implications**

The present review suggests some key messages for policy makers, safety practitioners, clinicians and other professionals concerned with children’s welfare. All such professionals should be trained to recognise how the internet and mobile technologies may be implicated in mediating or exacerbating risk of harm to children (Livingstone & Palmer, 2012). When clinicians and other professionals see a child showing signs of harm, they should inquire into the possible online as well as offline context in which the harm occurred, and not assume that understanding the offline circumstances will be sufficient to pinpoint or redress any and every problem. Although the relations among online and offline risks are not fully explored, offline risk, risk-taking or victimisation have an online dimension which should be considered when addressing the problem (Mitchell & Wells, 2007; Rice et al., 2012). It is important not to overreact to cases of online risk of harm by simply removing the child’s access to the internet or mobile phone. Not only will many children not report the online dimension of a problem for fear of losing their phone or computer but also those same technologies may be a source of private information, social support or other help to the child even as it brings risks.
Finding the balance between treating online risk seriously and yet not overreacting is difficult. A world without risk is undesirable, and 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); it is “a dynamic process encompassing positive adaptation within the context of significant adversity” (Luthar, Cicchetti & Becker, 2000: 543). Thus a risk-averse society, paradoxically, exacerbates rather than reduces the very vulnerabilities it seeks to protect by undermining the development of resilience (Gill, 2007; Green, Mitchell & Bunton, 2000). Moreover, one would misunderstand child development to suppose that, once adolescents become aware of the risks they will cease to take them.

The more children use the internet, and the more digital skills and confidence they gain, the more deeply and broadly they use it, thus encountering more risks as well as opportunities. One concern is that since children and young people’s experiences of opportunities and risks are positively correlated, efforts to reduce the latter may also reduce the former if policy interventions are not carefully designed (Livingstone & Helsper, 2010; Livingstone, Haddon & Görzig, 2012). Another concern is the ambiguity of many mobile and online activities: to upload new content, personal information must be disclosed; to find new friends one must make new contacts (‘strangers’); in exploring sexuality or health, one is likely to encounter pornographic or pro-anorexic sites.

It would require a further article to review the diverse and fast-developing array of policies, strategies and interventions designed to reduce harm by restricting risk or harm or enabling coping and resilience. Risk associated with mobile and online technologies is generally addressed by conducting an evidence-based risk evaluation (see Livingstone, Davidson, Bryce, Millwood Hargrave & Grove-Hills, 2012; O’Neill, Livingstone & McLaughlin, 2011; OECD, 2011; Savirimuthu, 2011; UNICEF, 2011). This is used to establish the legitimacy of certain risk management strategies, such as the development of regulatory institutions, the provision of user tools (Patchin & Hinduja, 2012; Slonje et al., 2013), peer mentoring (Kaanel-Platt & Douglas, 2012) or campaigns for awareness-raising. However, while weighing the merits and problems of possible interventions (including domestic filtering, parental mediation and education) is the focus of much public and policy deliberation, we conclude that, at present, the evidence base is too sparse for strong recommendations in favour of one approach over another.

For the most part, interventions have tended to address the youth (or parent) population en masse. What is required next is greater effort to tailor these interventions to
particular target groups, drawing on the research reviewed here regarding risk and protective factors. Jones, Mitchell, and Walsh (2013) reviewed internet safety education programmes, and point out the need for basing such programs on research findings, tailoring them to developmental needs, and evaluating their effectiveness. Much needed, and still little developed, is a body of research that conducts independent evaluations of existing interventions so as to learn from mistakes and share best practice (Perren et al., 2012). As an example, the KiVa antibullying program in Finland has been evaluated to reduce cyberbullying as well as traditional bullying (Williford et al., 2013). Insofar as the evidence base remains insufficient in pinpointing the conditions for and consequences of risk, the precautionary principle (Klinke & Renn, 2001) will continue to be invoked to justify policy interventions. We hope that this review will inspire researchers to fill the gaps identified above, developing the theoretical and empirical strengths of this emerging body of research to meet the undoubted challenges ahead.

**Supporting information**

Additional supporting information may be found in the online version of this article:

*Websites*

**General internet safety**

Child Exploitation and Online Protection Centre (CEOP): [http://ceop.police.uk/](http://ceop.police.uk/)
Crimes against Children Research Center: [http://cola.unh.edu/ccrc](http://cola.unh.edu/ccrc)
European Schoolnet: [http://www.eun.org/](http://www.eun.org/)
EU Kids Online: [www.eukidsonline.net](http://www.eukidsonline.net)
Safer Internet Centre (UK): [http://www.saferinternet.org.uk/](http://www.saferinternet.org.uk/)

**Cyberbullying**

BeatBullying: http://www.beatbullying.org/
Bullying statistics: http://www.bullyingstatistics.org/content/school-bullying-statistics.html
COST IS0801: http://sites.google.com/site/costis0801/
Cyberbullying Research Center (USA): http://cyberbullying.us/
Cyberbullying searchable information center: http://site.ebrary.com/lib/cyberbullying/home.action
DigitalME: www.digitalme.co.uk/
International Cyberbullying Think Tank: http://icbtt.arizona.edu/
KiVa program (Finland): http://bullyingandcyber.koinema.com/en/
Massachusetts Aggression Reduction Center http://webhost.bridgew.edu/marc/marc_research.html
Netsafe (NZ): http://www.cyberbullying.org.nz/

Acknowledgements
Sonia Livingstone’s work on this article drew on the work of the ‘EU Kids Online’ network funded by the EC (DG Information Society) Safer Internet plus Programme (project code SIP-KEP-321803); see www.eukidsonline.net. Peter Smith’s contribution drew on the work of COST Action IS0801 on Cyberbullying.

Correspondence
Sonia Livingstone
Department of Media and Communications
London School of Economics and Political Science
Houghton Street
London WC2A 2AE
Tel: 0207 966 7710
Email: s.livingstone@lse.ac.uk
Key points

- Usage by children and young people of mobile phones and the internet has increased dramatically this century; this is associated with a range of risks of harm.
- Many of these risks are aggressive (cyber bullying, cyber aggression) or sexual (pornography, sexting, stranger danger) in nature.
- Not all exposure to risk has harmful effects, but the evidence is growing of a range of harm associated with internet and mobile use, especially among vulnerable children.
- Online and mobile risks of cyberbullying, contact with strangers, sexual messaging (‘sexting’) and pornography generally affect fewer than one in five adolescents, depending on definition, sample and measurement.
- Prevalence does not appear to be rising with increasing access to mobile and online technologies, possibly because of the commensurate growth in safety awareness and initiatives.
- While not all online risks result in self-reported harm or upset, a range of adverse emotional and psychosocial consequences are revealed by longitudinal studies.
- The following risk factors are supported by evidence: personality factors (sensation-seeking, low self-esteem, psychological difficulties), social factors (lack of parental support, peer norms) and digital factors (online practices, digital skills, specific online sites).
- Key research gaps, and implications for practitioners, are identified.

References


Albury, K. (2013). Young people, media and sexual learning: Rethinking representation. Sex Education: Sexuality, Society and Learning, 13(S1), S32-S44.


and developmental disability in special educational settings. Developmental Neurorehabilitation, 12, 146-151.


OECD (2011). *The protection of children online: Risks faced by children online and policies to protect them.* Paris: OECD.


Ofcom (2012). *Children and parents: Media use and attitudes report.*


doi:10.1080/01411920903071918


doi:10.1177/0044118X12469379


