A Critical Perspective on Online Safety Measures

Elza Dunkels

PEER REVIEWED ARTICLE

Elza Dunkels
elza.dunkels@educ.umu.se

English abstract

The Nordic countries have enjoyed mass use of the Internet at home and in schools since the mid-1990's. Children have been noted to have rapidly taken the Internet into possession and to have made use of the affordances (Greeno, 1994) of Internet communication. However, media coverage of how children take on, and learn what the Internet has to offer has often been of a negative kind. Blazing headlines portray a generation in bottomless danger where children are defined both as possible victims and perpetrators. Another common attribute of this media coverage is the exoticising of young people's net cultures – describing the young and their cultures as profoundly different from earlier generations and elevating the "colourful and the bizarre" (Coffey *et al.*, 1999, p. 169) to a level where it appears normal for this particular generation. In this setting safe use guides – tips for parents and children on how to keep safe on the Internet – began to appear. They were often composed by teachers, concerned parents, non-governmental organisations and in some cases governments. The safe use guides were disseminated online in different forums aimed at concerned adults. In this article I will give a brief description of current online safety issues and examine them critically. My earlier research – 104 interviews with 12-year old Swedes conducted in 2004-2005 (Dunkels, 2007) and a study of European safe use guides conducted in 2008 (Lüders *et al.*, 2009) left me with a number of questions. I could see that safe use guides were strikingly similar, despite their origin, and I could see that they rested upon norms and values that were actually neither accounted for nor even declared. This article is a literature review of the area with the aim of critically discussing some of these questions.

Keywords: Online safety and risks, children, internet, literature review, cyberbulling and grooming.

Transforming Internet Use

The use of the Internet as an arena for communication has changed dramatically since the mid-1990s. In this section I will mention some of these changes that have had an impact on young people's use in relation to safe use guides. In the early days of Internet massification one of the most common applications was the open chat room, where you typically met strangers and talked to them (Sjöberg, 2002). Today these meeting places are mostly disregarded by young Internet users (Dunkels, 2007). Instead, we have seen the emergence of communications' tools that fill most of young people's interaction needs: the two most important ones being instant messaging tools and net communities. Both these types of interaction tools usually require members to log into their account before viewing other member's profiles and interacting with others, and this restricts the contacts to pre-defined friends or other, easily identifiable, members. The fact that young people today interact with those they already know from real life can be viewed as a general development of online interaction (Findahl, 2010). In the early days of Internet communication, much of the thrill involved merely being online, but today the communication tools have changed considerably.

Furthermore, Internet use has developed along two main paths; towards convergence and participatory content respectively (Jenkins, 2003). Convergence refers to the fact that many applications attempt to combine different tools so that the user needs to log in to fewer accounts. For example, a net community may provide multiple services such as chat, instant messaging, a blog, a notice board, e-mail and news feed. Moreover, some completely new tools have emerged, tools whose only function is to combine the user's different interaction applications. This means that the user can log into one single account to reach all her accounts. The appearance of participatory content refers to the increased possibilities for creating and disseminating material over the Internet. The Internet has made it easier and cheaper to publish information, but it is only in the 2000's that publishing has become accessible to practically any Internet user. The emergence of web interface publishing, where blogs feature heavily, combined with steadily decreasing prices for personal computers, has paved the way for a mass movement in publishing one's own material. This can be understood as one of the affordances of contemporary media that young people to a great extent have identified and made use of; young people are creating texts, music, films and more (Veen & Vrakking, 2006; Ito *et al*, 2008). The Internet has developed from being an extension of traditional media, where transmitters and receivers were clearly identifiable parties, towards a more complex structure where amateurs also can be producers (van Dijck, 2009).

Children and the Internet

Children's living conditions can be described using the intersection of parameters such as age, gender, social class and ethnicity. This applies to any age, but age as a systemic parameter becomes especially interesting when we discuss risks on the Internet because of the persistent notion of a generational gap. The construction of childhood (James & Prout, 1997) as a separate and distinguishable part of life underpins the concept of generational differences. Prensky (2001) introduced the expressions digital natives and digital immigrants to portray the different generations' different attitudes towards the Internet. This difference can also be detected in the many other attempts to label the young in relation to technology. The young have been given epithets such as the Electronic Generation (Buckingham, 2002), the Net Generation (Tapscott, 1998) and Homo Zappiens (Veen & Vrakking, 2006). Prensky's dichotomy of natives and immigrants has been criticised by, among others, Bayne & Ross (2007) for simplifying the matter and for stressing the differences too much. My interpretation of Prensky's idea is that the metaphor serves as a pedagogical

aid to help us understand; by applying knowledge we already have, concerning a well-known area, we can more easily understand this new area. Prensky argues that the digital immigrants should take on the perspective of the natives and make use of their knowledge in order to improve the educational system. Other researchers, such as Tingstad (2003), Veen & Vrakking (2006), Dunkels (2007) and Moinian (2007) have also stressed the importance of trying to view contemporary phenomena from the vantage points of the young users. Herring (2008) even calls for a paradigm shift in this kind of research, stressing the need for both a change in methodology and for contextualised interpretations (see also Sjöberg in this volume).

Using the generational angle is enticing when you analyse the different conditions under which the generations have been brought up. Digital natives and digital immigrants can be useful images to describe differences but they hide the dividing factors within the generations; skills and access to computers and the Internet can differ very much. Bennett *et al.* (2008) argue that there is no real support for the claim that knowledge of contemporary technology is universal and comparable among the younger generation. They refer to research that implies that there are in fact potential differences in skills that can be ascribed class, gender and ethnicity. Furthermore, from von Feilitzen's research overview from 2009 it is clear that the Internet is not one medium, in the sense of old mass media, but rather a diverse, almost limitless, medium which is hard to describe using existing terms. von Feilitzen's (2009) overview also emphasises the fact that Internet users can take on different roles; producer, consumer, participant. Such a diversified area as IT thus calls for an extreme variety of skills; it is not possible to master IT as a whole. There can be skills in the technology itself, artistic expression, learning, teaching, communication, to mention a few diverse areas. These skills may differ between and among generations, along with different views of contemporary phenomena. Larsen (2008) gives an example of how a young girl publishes her portrait on a website aimed at her closest friends. Adults view this as a potential risk since they identify the infinite audience for her portrait. Larsen explains this using Scollon's *geographies of discourses* to label the girl's actions as local; aimed at her friends and the adults' actions as global; they worry that the entire world might see the image. This discrepancy between the actor's intentions and the surrounding world's understanding of it is also described by Nigård (2009). Nigård interviewed young people about their publishing of self portraits with sexual connotations and in many cases the young person and her audience had very different views and expectations in relation to the same incident.

Understanding how the different views of adults and children may lead to questions of power – power to speak and power over resources. Children are often represented and spoken for (Oswell, 1999), but we very seldom create arenas to give voice to them. In this context the Internet may be interpreted as an arena for expression and as such an arena of unusually widespread access. Hernwall (2003) also points out that the Internet can become an arena for transgressing physical boundaries, such as age. Furthermore, Internet access is a question of economic and infrastructural resources and as Jones (2008) points out, children are dependent on family resources, but they have no control over these resources. An emerging academic interest is that of childism (Alderson, 2005), a perspective that recognizes power structures concerning age similar to those we acknowledge regarding gender and ethnicity (Dunkels, 2007). When age and power are intersected in this way, new questions and academic challenges appear. The power dimension can thus be seen as a back-drop for the concepts of online safety, discussed in the following section.

Online safety?

History shows that mass use of a new medium is followed by an emotional reaction. These emotional reactions, called media panics (Drotner, 1999), technopanics (Marwick, 2008) and moral panics

(Springhall, 1998) typically express anxiety over young people's use of some new technology. A vital part of these reactions is to list the possible risks of said medium and consequently list appropriate safety measures or strategies. The same development can be seen regarding young people's Internet use. In this article risk is defined as possible negative outcomes and safety measures or strategies as actions undertaken to avoid or counteract risk.

Preventing risks on the Internet has been a task assumed by governments, educational institutions and non-governmental organisations such as The Red Cross and Save the Children. It is possible to divide safety strategies into three, partly overlapping, main levels: legal, infrastructural and personal. At the legal level several steps have been taken to update legislation in accordance with technological developments such as finding solutions to file sharing issues, finding ways to prevent adult predators from pursuing victims and regulating how personal data may be handled. At the infrastructural level, legal and self-regulation measures have been taken to stop illegal and unethical use of the Internet; two examples are child pornography filters and surveillance of data traffic. At the personal level the safety strategies have targeted possible victims and perpetrators with regulations and information campaigns. For this article the third, personal, level is the most relevant, which is why the focus will be on safety strategies directly aimed at children and parents. There has in fact been clear family focus on how the questions of personal online safety are addressed, defining parents as the natural level of responsibility. Therefore many of the safe use guides that have been published since the mid-1990's target parents and children as actors.

Any safety strategy is based on calculations of risk; how grave is the danger, how much freedom can be sacrificed in relation to how much is to be gained. To underpin these assumptions we must therefore ascertain under what circumstances Internet use becomes unsafe. As an example, the Eurobarometer (European Commission, 2008), lists five possible strategies for parents supervising their children's Internet use: staying nearby whenever the child is online, checking their child's e-mail or instant messaging account, specifying rules for their child's Internet usage, installing filtering software and installing monitoring software. A number of implicit ideas underpin this listing and I will give two examples. First, the fact that supervising is mentioned as a strategy in the first place suggests a family construction in which parents and children have a supervisor-supervised relationship. Secondly, the idea of parents' legal and ethical rights to access a child's e-mail and instant messaging account is a prerequisite for the listing. Thus, the way we talk about and practice online safety reveals how we view children and childhood.

A growing area of research is interested in whether a safety strategy actually makes sense in the context of young Internet users. As an example the Swedish Data Inspection Board (2009) national survey of 14-18-year olds reveals that only 25% of them use the abuse function on social networking sites. The abuse function is a tool that content providers have agreed on placing on every page of young people's online meeting places. According to the Swedish Data Inspection Board these low figures speak against other results confirming that the abuse function is in fact an efficient tool since only 15% reported "it didn't work sufficiently or that nothing happened after it was used" (Swedish Data Inspection Board, 2009: 9). However, there is another possible explanation for the figures not corresponding to each other – the abuse function may be seen as meaningless because there are other safety strategies that work better. We cannot therefore conclude, from the evidence presented in the report, that young people "engage in unsafe behaviours" (Ibid.: 3). Instead, it could prove useful to attentively study young people's net cultures with the ambition to understand it from the views of the young and carefully avoid considering the adults' views as the norm (see also Sjöberg in this volume).

As will be discussed below, the different meanings of the word *safety* can be responsible for some of the confusion we see today. For example, the Swedish Data Inspection Board (2009: 9) claims that the majority of young people "do not adapt their behaviour according to the risks." As non-risky behaviour the report mentions encrypting e-mail addresses and e-mails. This claim is made although there is no evidence that the listed behaviours actually constitute a risk. In fact, we know very little of what constitutes personal risk online. It seems that some postulations from the early Internet massification days were nothing more than assumptions, based on hypotheses concerning online interaction that still remain to be proved. One of these hypotheses concerns sharing personal information; it was said to be hazardous to share personal information such as "messenger id, e-mail address, mobile number and any pictures of you, your family or friends" (Think U Know, 2009). Online anonymity is in fact still one of the most widespread requests in safe use guides (Lüders *et al.*, 2009). However, there seem to be problems with safe use guides as they are formulated today. One problem is that there is no proof of any correlation between divulging personal information and online risk. Another is that some of this advice might in fact be counterproductive. Staksrud *et al.* (submitted) and Brandtzæg (2009) claim that anonymity can make some children reveal more information than they normally would have, thus creating a potentially more dangerous situation than if the interaction had been open. Because of inherent characteristics of computer mediated interaction, which Suler (2005) calls *the online disinhibition effect*, children may act in a less inhibited fashion when the online setting decrees anonymity. This disinhibition can in turn lead to risky behaviour, children possibly divulging to potential perpetrators that they are unhappy, attention-seeking, etc. Along the same lines Shifman & Varsano (2007) analysed what they call "clean joke" websites – websites that have been filtered for certain content in order to make them appropriate for children and young people. Their conclusion is that letting children use clean joke websites may be even more dangerous than letting them use non-filtered sites, since the idea of clean jokes "encourages parents to let down their guard and be less critical about the values to which they expose their children" (Shifman & Varsano, 2007, p. 8). These researchers imply that some safety strategies undertaken by adults cannot only be ineffective, but even counterproductive and thus work against their goals. Some informants in my study of 12-year olds (Dunkels, 2007) claimed that they would not tell their parents if anything unpleasant happened, because they then would risk that their parents, out of concern, would shut them off the Internet. This incites the question of whether the safe use guides can in fact become counterproductive. These are important results that urge us to carefully consider safety measures and make sure that they are meaningful for young Internet users.

Risk and Safety: definitions

In order to understand online risk and safety we need to problematize these two concepts, both of which have been used quite freely, without actual definitions.

Risk can be seen as a social construction and at the same time as an objective reality and thus something that changes over time and between cultures. The notion of risk is highly connected to the values and perceived norms of the individuals and groups that discuss it. For example, the perception of how much and what information you share with others may very well vary among cultures, countries and groups of people. On the other hand it might be possible to find risks that are recognised as risks by practically anyone such as sexual assault, theft and corporal and mental abuse. Therefore when discussing risks we must make certain that we agree on what constitutes a risk and, moreover, that we understand that risk is not a cross-cultural and fixed concept. This is not to say that the conception of risk is in constant flux or to play down the grave dangers facing children online on a daily basis. Rather, it is to emphasise the importance of continuously discussing

the notion of risk so that we are not tempted to think that we can reach consensus effortlessly. Yet another problem with the concept of risk is taken up by Sharples *et al* (2009) who point out that there can be a difference between likely risk and worst-case risk. This distinction is however seldom seen in media reports on children and the Internet.

Safety is another issue that has confusing semantics attached to it. Safety has been used to label very different concepts such as technical safety and personal safety. Technical safety is an area that deals with data viruses and firewalls, where the problems are of a technical nature, while personal safety refers to privacy issues and how to avoid being harmed or deceived online. The recommendations for young people's Internet safety will thus differ depending on whether we define safety as technical or personal. Oswell (1999) argues that the apparent straightforwardness of the question of how to protect our children online, in fact conceals the question of who really has the right to be concerned about these questions when the problems and their solutions are defined.

Children at risk

Children's Internet behaviour has been a subject of adult interest since the early Internet massification in the mid-1990s. To some extent the reactions to young people's Internet use have been emotional, portraying a dystopic future and all children as potential victims. These emotional responses have been labelled media panics by Drotner (1999) who, among others, claims that this is a recurring phenomenon that unavoidably follows the introduction of new media. Drotner also argues that as a group we suffer from historical amnesia – we fail to learn from what earlier technology shifts might teach us – and so history repeats itself with every introduction of a new medium.

The European Union funded project EU Kids Online deals with safety and risks concerning young people and new media (Hasebrink *et al.*, 2008). Some of the risks listed are illegal content, paedophiles and grooming, harmful or offensive content, cyber-bullying, stalking, harassment, gambling, financial scams, invasions or abuse of privacy. The European Commission (2008) further divides the risks into illegal material and harmful material, to stress that these are not necessarily the same. However, Oswell (1999) claims that the European Union overlooks the fact that problematic content can be divided into a number of sub-groups. The most obvious is content that harms children when they consume it, but Oswell also identifies four other kinds of problematic content. First there is content that incites the consumer to harm children and second content that harms children in the process of production. Both of these can, for example, contain child pornography; in the way that this content can provoke adults to abuse children and that the production process itself typically constitutes sexual abuse towards a child. In the third group we have, for example, discrimination, content which is harmful because of its very nature, no matter what, or even if it has an effect. The fourth group is content which is "harmful to the child neither in the context of production nor consumption, but which constitutes a violation of the image of the child (e.g., morphing images of children in sexually explicit situations)" (Oswell, 1999, p. 45). In the following I will illustrate online risk by using two of the risks mentioned in Hasebrink *et al.* (2008): cyber bullying and grooming.

Cyber Bullying

Cyber bullying has been in the headlines as a threat since the late 1990's. Shariff (2008) lists some important and distinguishing characteristics of cyber bullying:

- Anonymity; the Internet allows for the targeting of victims without being easily detected. The bully's true identity can be hidden by screen names.
- An infinite audience; the possibility for hundreds of bullies and bystanders to get involved in the abuse.
- Permanence of expression; abusive materials are difficult to remove once published online.

However, these traits of cyber bullying might not be as distinguishing as they may first seem. For instance, there may be a difference between actual anonymity and perceptible anonymity (Dunkels, 2007). Looking at the Internet use patterns of young people, many online contacts are the same as real life contacts; the parties are known to each other also in the traditional sense. It is in fact quite uncommon to have mostly strictly online contacts even though there are some who for different reasons mostly connect with formerly unknown people. This is in agreement with the altered communication patterns, from the more random connections of the 1990s to the more deliberate links of today. So the anonymity issue might not be as strong today as it was ten years ago. Furthermore, the notion of an infinite audience needs problematisation, because we do not know for a fact that an infinite audience is actually larger than a fixed audience. To clarify, we do not know from empirical evidence that someone who is not connected in any way to the victim is as interested in watching the documented bullying incident as someone who actually knows the victim. Therefore, we cannot conclude that the audience is bigger only from the fact that the possible audience is bigger. There are, no doubt, documented incidences where the audience of a bullying incident has become gigantic, with severe consequences for the victim. One example of this is the story of the Star Wars Kid (Wikipedia, 2009), a 14-year-old boy whose homemade film of himself acting out a scene from the movie Star Wars became one of the most popular films on the Internet that year. The boy was harassed by his school mates and unknown people from all over the world and his parents eventually filed a lawsuit against some of the children at school (Globe & Mail, 2007). However, these stories constitute a few exceptional cases and it is too early to say that the Internet has actually changed the conditions for bullying on more than a superficial level. The fact remains that whenever a child is bullied, regardless of the geographical or technological context, it is a personal tragedy for the victim and a situation that society generally does not accept. The case mentioned above also illustrates the fact that not only does the bullying incident or the abusive material have a potentially larger audience, but also that the information that someone is bullied can be disseminated to a potentially larger group. The permanence of expression can be seen as continuous abuse as every time someone sees the abusive material this can be regarded as further abuse. There is also another side to the permanence of expression; this condition can be exploited in order to document incidences or proof of incidences for legal or other processes. This circumstance can be interpreted as yet another affordance of contemporary media, and some schools have in fact identified and made use of this to follow up on bullying and harassment among their pupils.

Grooming

Grooming refers to the risk of adult predators seeking contact with possible victims online. Today we know from the research of Shannon (2007) and Ybarra *et al.* (2007) that many of the victims of sexual assault following an online contact already had a troubled real life situation. Many of the victims lacked parental or other adult support or had a history of being bullied at school. In fact, recent research has shown that the most probable scenario is one where the perpetrator takes advantage of the fact that the child needs adult support and attention. Typically, the predator contacts children who reveal their vulnerability online and then offers to become the adult they seek,

slowly building up a manipulative relationship with the child (Shannon, 2007). The first few contact attempts usually concern everyday topics that anyone could talk about. When this process of preparing for a crime – grooming – is completed, the potential victim often readily travels to meet the predator with whom they think they have a parent-child or friendly relationship or even romantic involvement. In practice, this means that often the deception is on the level of the perpetrator's agenda, not on his identity. The predator can be honest regarding his age and name, but sometimes deceives the child when it comes to his intentions with the relationship. Ybarra & Mitchell (2008) claim that close to four out of five cases reveal that the perpetrators are truthful regarding their intentions to have sex with the young person concerned. This knowledge of the grooming process is in stark contrast to the early assumptions of what could constitute an online threat. In fact, many of the warnings still presuppose courses of action that are very rare such as a child being deceived regarding the age and sex of the offender or an offender seeking out a child in real life that he has found pictures of online. Naturally, there will always be cases that are not typical. However, this knowledge of how abuse in general occurs can be useful for underpinning safety strategies, which are discussed in the next section.

Safety Strategies

It is possible to distinguish between two different levels of safety strategies; where children are objects and subjects respectively. The first is aimed at young people, but formulated by adults; the second level is young people's own safety strategies. In the first category one of the most widely spread safety measures is content filters for personal and public computers. Filters can be built on different algorithms that filter words, images, meta-data or a combination of these. Another safety strategy involves compiling white lists of approved websites or other media content. Blacklisting is yet another method, where the list comprises content that should be avoided. In all these cases the strategy is to help parents, teachers and other adults to act in a responsible way and to be able to guide children in their Internet use. Whatever the method of filtering or attempting to compile white or black lists, some basic issues will remain according to Price & Verhulst (2005). First of all the user will have to select filtering criteria and the lists to choose from will need to be very long if they are to fit all kinds of family structures, cultures, ideologies, etc. Secondly, whatever content is to be filtered out is subject to ideological biases, recognised or not by the users. This is a consequence of the fact that the software needs to be fed with parameters to be of any use. These parameters will have to be set by humans at some point, humans who have to decide whether different types of content are appropriate for children or not. These decisions and their consequences are not likely to be displayed for the user and so the software user has to trust the ideology of the producer. Thirdly, because the filters will provoke content providers to circumvent them using all possible means, there is a risk that small, non-commercial content providers may have trouble coming through the filters or white lists and thereby become "silenced" (Price & Verhulst, 2005, p. 128). This silencing becomes even graver since the Internet may be the only channel of public expression accessible for the small, non-commercial content providers.

Self-regulation – the industry taking on responsibility – is a wide-spread method of preventing risk. As an example, the European Union countries have the Pan European Game Information system – PEGI – that aims to "help European parents make informed decisions on buying computer games" (PEGI, 2009). The PEGI system classifies computer games into eight so-called descriptors: violence, bad language, fear, drugs, sexual content, discriminating content, gambling and whether the game can be played online with other people. Any classification will rest upon a set of values, or as Oswell (1999) puts it "classifications are derived from particular normative (and normalizing) discourses of

the child and family" (Oswell, 1999: 51). According to Shifman & Varsano (2007) this is a general problem with this kind of voluntary gate keeping because the criteria for selection are very rarely transparent and the users are thus left to rely blindly on the gate keepers. Another more general problem is that content in many cases is perceived in different ways by different individuals, making gate keeping hard if not impossible.

When it comes to children's own safety strategies there are very few studies. My study (Dunkels, 2007) describes the well-functioning safety strategies that most children have. It is noteworthy that these strategies were developed by the children alone at the computer or together with peers. Teachers and parents were conspicuous by their absence in this study, which is one of the few that have actually focused on children's views on online risks. Furthermore, it was clear that the risks expounded in the media were not present in the children's everyday lives. They knew of them by reputation only and were never really exposed to the grave dangers such as cyber bullying and grooming. The study paints a positive picture of competent young citizens who have learned how to avoid what they themselves define as negative on the Internet. However, we do not know for a fact that these counter strategies actually work should something serious occur. Since the strategies were developed practically without adult input it is possible that the children did not actually make informed decisions when they encountered what might have represented a risk. This lack of research regarding children's own safety measures is also pointed out by Livingstone & Haddon (2009). Basically the same stance is taken by Ybarra & Mitchell (2008: 352) when they say that

> *Thoughtful approaches to prevention that focus on children's behaviors online (e.g., harassing others) and their general psychosocial profile (e.g., aggression problems or depressive symptomatology) instead of particular technologies (which will continue to evolve into new and more interactive applications) are needed.*

There is some emerging research on what actually constitutes online risk, such as Staksrud (2009) claiming that the children who have the least practice and competence concerning the Internet are the most exposed to unwanted experiences online. This calls for more research and more critical questions since it in many ways contradicts general beliefs about children and online safety.

Conclusions

Above I describe how the discourse surrounding online risk has developed since the early days of Internet massification. From the first general assumptions, based on adult interpretations of this new medium, via the first studies, to an emerging insight that contextualisation is needed. The contextualisation – taking in the young user's own view when analysing contemporary media – implies that the question of how to counteract online risk for children is more complex than some of the solutions suggest.

One might describe the present knowledge of online risk as immature, still in its early formative phase. So, in order to understand this area we need to problematise the concepts of risk and safety which up until now have been used quite freely, without actual definitions. We need to contextualise these concepts in relation to how children are constructed in society. This might lead to discovering that legal and ethical expressions rest upon different constructions of childhood. We need to discuss what these expressions actually say about the child, childhood and the family; is the child seen as a competent citizen, is the family constructed hierarchically, is childhood regarded as a state of becoming rather than being? This kind of analysis of the basis for different safety measures can be

one way of addressing the important questions of children's online safety. Our choices of safety measures are underpinned by our views of children, childhood and family and this fact needs to be addressed.

We also need to acknowledge that any gate keeping, self regulation, filtering or classification is underpinned by a set of values. Not only is this important to discuss in our increasingly global and diverse society, but just as much in communities that appear homogenous. In countries or cultures that appear uniform there will still be different views and values. In an apparently diverse society the different vantage points are more obvious, but they are just as important to discuss when the de-construction of implicit norms and values is not as transparent.

The notions of risk, safety, childhood and even family as social constructions, possible to de-construct and question, contradict the concept of compiling lists to fit all. Hence, the extensive listing that continues on a government level, among non-governmental organisations and down to educational institutions may be questioned. Safe use guides, white lists, black lists, computer game classifications are all crude instruments. Furthermore, there is a risk that these crude instruments could become counterproductive and provoke children to hide their online behaviour from adults.

References

Alderson, P. (2005). Generation Inequalities. UK Health Watch 2005: 47-52.

Bae Brandtzæg, P. (2009) Privat 2.0 In Grande Røys, H. (Ed.) Delte Meninger. Oslo: Universitetsforlaget.

Bayne, S. & Ross, J. (2007) The 'digital native' and 'digital immigrant': a dangerous opposition. Paper presented at the Annual Conference of the Society for Research into Higher Education (SRHE) December 2007.

Bennett, S., Maton, K. & Kervin, L. (2008) The 'digital natives' debate: A critical review of the evidence. British Journal of Educational Technology, 39(5): 775-786.

Buckingham, D. (2002) The Electronic Generation? Children and New Media. In Leah Lievrouw & Sonia Livingstone (Eds.), The Handbook of New Media. London: Sage.

Coffey, A., Holbrook, B. & Atkinson, P. (1999) Qualitative Data Analysis: Technologies and Representations. In Alan Bryman & Robert Burgess (Eds.), Qualitative Research. London: Sage Publications.

Drotner, K. (1999) Dangerous Media? Panic Discourses and Dilemmas of Modernity. Paedagogica Historica, 35(3): 593-619.

Dunkels, E. (2007) Bridging the Distance – Children's Strategies on the Internet. Umeå: Umeå University.

European Commission (2008) Eurobarometer: Towards a safer use of the Internet for children in the EU – a parents' perspective. European Commission.

Findahl, Olle (2010) Unga Svenskar och Internet 2009. Stockholm: SE (Stiftelsen för Internetinfrastruktur).

Globe & Mail (2007-04-07) 'Star Wars Kid' cuts a deal with his tormentors. www.theglobeandmail.com/servlet/story/RTGAM.20060407.wxstarwars07/BNStory/National/home

Greeno, J. (1994) Gibson's affordances, Psychological Review, 101(2): 336-342.

Hasebrink, U., Livingstone, S. & Haddon, L. (2008) Comparing children's online opportunities and risks across Europe. Available at www.eukidsonline.net.

Hernwall, P. (2003) Barn@com Stockholm: HLS Förlag.

Herring, S. (2008) Questioning the Generational Divide: Technological Exoticism and Adult Constructions of Online Youth Identity. In Buckingham, David (Eds.) Youth, Identity, and Digital Media. Cambridge: MIT Press.

Ito, M., Horst, H., Bittanti, M., Boyd, D., Herr-Stephenson, B., Lange, P., Pascoe, C. J., Robinson, L., Baumer, S., Cody, R., Mahendran, D., Martínez, K., Perkel, D., Sims, C. & Tripp, L. (2008) Living and Learning with New Media: Summary of Findings from the Digital Youth Project. Chicago: MacArthur Foundation.

James, A. & Prout, A. (1997) Constructing and Reconstructing Childhood: Contemporary Issues in the Sociological Study of Childhood. London: Routledge.

Jenkins, Henry (2003) Quentin Tarantino's Star Wars?: Digital Cinema, Media Convergence, and Participatory Culture. In Thorburn, David, Jenkins, Henry & Seawell, Brad (2003) Rethinking Media Change: The Aesthetics of Transition.

Jones, G. (2008) Youth, Citizenship and the Problem of Dependence. In Invernizzi, A. & Williams, J. (Eds.) Children and citizenship. London: Sage.

Larsen, M. (2008) Online Social Networking: From Local Experiences to Global Discourses. Paper presented at Internet Research 9.0: Rethinking Community, Rethinking Place, The IT University, Köpenhamn 20081015–18.

Livingstone, S. & Haddon, L. (2009) Opportunities and Risks for European Children. In Young People in the European Digital Media Landscape. Gothenburg: Nordicom.

Lüders, M., Bae Brandtzæg, P. & Dunkels, E. (2009) Risky Contacts. In Livingstone, Sonia & Haddon, Leslie (Eds.) Kids Online: Opportunities and Risks for Children. London: Policy Press.

Marwick, A. (2008) To catch a predator? The MySpace moral panic, First Monday, 13(6).

Moinian, F. (2007) Negotiating identities: exploring children's perspectives on themselves and their lives. Stockholm: LHS.

Nigård, P. (2009) Frivillig sexuell exponering på nätet. In Se mig – unga om sex och internet. Stockholm: Ungdomsstyrelsen.

Oswell, D. (1999) The Dark Side of Cyberspace: Internet Content Regulation and Child Protection. Convergence, 5(4): 42-62.

PEGI (2009) Pan European Game Information www.pegi.info/en.

Prensky, M. (2001) Digital Natives, Digital Immigrants. On the Horizon, MCB University Press, 9(5).

Price, M. & Verhulst, S. (2005) Self-regulation and the Internet. The Hague: Kluwer Law International.

Shannon, D. (2007) Vuxnas sexuella kontakter med barn via Internet. Stockholm: Brottsförebyggande rådet.

Shariff, S. (2008) Cyberbullying. Issues and solutions for the school, the classroom and the home. New York: Routledge.

Sharples, M., Graber, R., Harrison, C. & Logan K. (2009) E-safety and Web 2.0 for children aged 11–16. Journal of Computer Assisted Learning, 25: 70–84

Shifman, L., & Varsano, H. M. (2007) The clean, the dirty and the ugly: A critical analysis of 'clean joke' Web sites. First Monday. www.firstmonday.org/issues/issue12_2/shifman/index.html

Sjöberg, U. (2002) Screen Rites: a study of Swedish young people's use and meaning-making of screen-based media in everyday life. Lund, Lunds universitet.

Springhall, J. (1998) Youth, popular culture and moral panic: penny gaffs to gangsta-rap, 1830-1996. Basingstoke: Macmillan.

Staksrud, E. (2009) Hva slags barn vill vi ha? In Grande Røys, H. (Ed.) Delte Meninger. Oslo: Universitetsforlaget.

Staksrud, E., Bae Brandtzæg, P, Hagen, I. & Wold, T. (2009) Children's experiences of cyberbullying and harassment in different technological platforms, Journal of Children and Media, (): 349–365.

Suler, J. R. (2005) The online disinhibition effect. International Journal of Applied Psychoanalytic Studies 2(2): 184-188.

Swedish Data Inspection Board (2009) Youth and Privacy 2009. Stockholm: Swedish Data Inspection Board.

Tapscott, D. (1998) Growing Up Digital: The Rise of the Net Generation. New York: McGraw-Hill.

Think U Know (2009) Internet Safety Tips. www.thinkuknow.co.uk/11_16/topten.aspx

Tingstad, V. (2003) Children's chat on the net. A study of social encounters in two Norwegian chat rooms. Trondheim: NTNU.

van Dijck, José (2009) Users like you? Theorizing agency in user-generated content. Media Culture Society 31:41.

Veen, W. & Vrakking, B. (2006) Homo Zappiens – Growing up in a digital age. London: Network Continuum.

von Feilitzen, C. (2009) Influences of Mediated Violence. Gothenburg: The International Clearinghouse on Children, Youth and Media.

Wikipedia (2009) Star Wars Kid, en.wikipedia.org/wiki/Star_Wars_kid

Ybarra, M. & Mitchell, K. (2008) How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs. Pediatrics, 121(2): 350-358.

Ybarra, M., Mitchell, K., Finkelhor, D. & Wolak, J. (2007) 'Internet Prevention Messages: Targeting the Right Online Behaviors', Archives of Pediatrics & Adolescent Medicine, 161(2): 138-145.