Author version of the paper

Children and web 2.0: What they do, what we fear, and what is done to make them safe

Hartikainen Heidi, Iivari Netta, Kinnula Marianne
University of Oulu

Abstract. Children of today start using Internet earlier and earlier and this has gained attention of scholars in various disciplines such as psychology, sociology, and media. Concerns about children's online safety have increased but Information Systems (IS) research on this area is still scarce even though information security is an established field of research within IS research. In this paper we review the existing research on children's online activities and related threats and risks, as well as initiatives to achieve online safety. We identify gaps in current research, including lack of qualitative studies and research related to young children, and lack of research addressing the effectiveness of educational initiatives. We also argue that IS research should contribute to this research field by studying children's information security and privacy related behavior and different available trainings. After all, good information security skills lay the groundwork for privacy, the cornerstone for online safety.

Keywords: Online safety, information security, web 2.0, social web, social media, media skills, education, children.

1 Introduction

The term Web 2.0 (or social web) is used to describe a new generation of web development facilitating collaboration, interactivity, end user contributions, and information sharing [41]. Social media is a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, allowing (co-)creation, sharing, discussing, and modifying of user generated content [19], [20]. Examples of social media include *blogs or microblogs* like Tumblr or Twitter, *social networking services* like Facebook and Google+, *virtual gaming worlds* where you interact with others like World of Warcraft, *virtual social worlds* like Second Life, *content communities* like YouTube, Flickr and *collaborative projects* like Wikipedia [19]. The core of social media is in "one-to-few" or "one-to-many" communication [22]. This often contains sharing private information like gender, age, address, phone number, photographs etc., despite concerns related to privacy issues [31]. Furthermore, younger users share more information about themselves than older users [31].

The users of web 2.0 and different social media services are getting ever younger [26]. Children grow up in an increasingly digital world and their communication, socialization, creation, and learning processes are strongly affected by technology

Hartikainen, Heidi, Netta Iivari, and Marianne Kinnula. "Children and Web 2.0: What They Do, What We Fear, and What Is Done to Make Them Safe." *Nordic Contributions in IS Research*. Springer International Publishing, 2015. 30-43.
Published in the 6th Scandinavian Conference on Information Systems (SCIS) 2015.

[35]. Children are increasingly surfing the web [30] and social networking sites, playing online games, and using video sharing sites, and gadgets like iPods and mobile phones are well-established fixtures of youth culture [18]. The term "digital native" was coined to describe children that have grown up "surrounded by and using computers, video games, digital music players, video cams, cell phones and all of the other toys of the digital age" [34]. As the Internet and social media have truly entered the lives of today's children, concerns about children's online safety are also growing.

In addition to parental concerns, online safety of children is an area that has raised much academic interest within diverse set of disciplines, such as media and communication studies, psychology, pedagogy and sociology. While information security is an established field of research within Information Systems (IS) research, children and their information security and online safety concerns, however, have remained so far neglected in IS research. Information security within IS research is usually interpreted as securing confidentiality, integrity and availability of information [11] and the IS community has studied social media and different privacy and safety issues involved, mainly focusing on adults [8], organizational aspects [13] or technological developments [27]. However, information security and online safety of children are valid concerns also for IS researchers and this study will map the field for the IS researchers to enter into. This mapping is quite a complicated as these topics have been studied within various disciplines due to which it was necessary to review a multidisciplinary body of research. The review is further complicated by the fact that online safety is a diverse and relatively new research field without widely accepted theoretical frameworks or standard methodologies, and where definitional, measurement and interpretative challenges still prevail [26].

In this paper we set out to produce an understanding of the state-of-the-art of research on children's online safety. This will be accomplished by first reviewing research on children's online activities, showing the relevance of social media in their lives, then moving on to research reporting threats and risks associated with children's online activities, and ending up with reviewing research on the different initiatives taken to secure children online. A special focus will be paid on studies carried out in Finland, the context in which the empirical part of this study will be later carried out. Finland has been categorised as a 'high use' country in terms of its young people's Internet habits, similar to the case of other Nordic countries [9]. However, literature on the topic will be included also from other countries and the results should be utilizable by researchers interested in the topic in general.

The paper proceeds as follows: First, the methodology for the literature review is presented. After that we go through children's online activities, the threats that they might face as well as the efforts that have been introduced to ensure their online safety. The last chapters feature discussion of our results and conclusions.

2 Methodology

There are different types of literature review, i.e. the traditional (narrative) method, the systematic method, meta-analysis and meta-synthesis. In this paper we are using a traditional narrative literature review method. Even though we recognize that for example the systematic literature review (SLR) is gaining popularity in the IS field

[2], we believe that a narrative method is more suitable for this paper as our aim is "to gather together a volume of literature in a specific subject area and summarizing and synthesizing it" [5]. A narrative literature can inspire research ideas by identifying research gaps and inconsistencies [5] whereas in SLR the aim is usually to address "highly specific research questions for which evidence from literature is sought" [2].

Three strategies were employed to collect the literature reviewed in this paper. First Google Scholar services were used to search with keywords and phrases such as social media, children, online safety and information security as well as different variations of those. Second, databases such as Scopus, ProQuest and Web of Science were used to perform searches with same terms. An example search carried out in the Scopus database is as follows: (TITLE-ABS-KEY ("social media" OR facebook OR instagram OR twitter OR "social network" OR sns OR internet OR www) AND TITLE-ABS-KEY ("information security" OR privacy OR trust OR "cyber security" OR "internet security" OR "online safety") AND TITLE-ABS-KEY (child* OR youth OR young OR kids OR adolescent* OR "digital native*") AND TITLE- ABS-KEY (training OR education OR "awareness building")). Finally, additional literature was obtained by going through the reference lists of relevant articles acquired in the previous phases. The search was performed in articles written in English and Finnish, but it was not limited to specific journals, conferences or databases as the aim was to try and get as rich as a picture as possible. Publication years of the articles were not limited.

During three months, a total of 318 articles or book chapters were collected and organized into a RefWorks database together with information such as author name, name of the article, publication dates, journal name, abstract, purpose of the research, and information about the research design. The references were also extracted through RefWorks to an easily manageable excel file weekly and a paper trail of searches was kept to avoid repeating the same tasks and searches during the process. Finally a narrative synthesis of the materials was done with the purpose of providing the reader an easy to read background for understanding current knowledge in the area and highlighting the significance of new knowledge [5].

3 What do children do online?

The Internet and mobile and online technologies have opened up a world of possibilities for children, expanding their horizons and providing opportunities to learn, create identities, and participate in society [7], [26]. The number of online activities young people engage in increases with age and years of Internet use [26].

The most popular online activities among children are use of Internet for schoolwork and playing games on your own. Watching video clips is also popular as well as instant messaging, sending and receiving emails, and visiting social networking sites. The more active Internet users also engage in playing games against others, download music or films, post photos, use webcams, or post messages on websites. Visiting chat rooms, spending time in virtual worlds, or writing a blog or a diary are practiced only by a smaller percentage. [12]

Finnish children have a lower number of online activities than children in Europe on average, even though their daily use of the Internet is much higher than European

average. The most popular Internet activities among Finnish children are playing games alone, watching video clips, receiving and sending email, using the Internet for schoolwork, and visiting social networking sites. [9]

Online activities of children have also been divided into three genres of participation that describe young people's engagement with new media: *Hanging out* refers to friendship driven participation corresponding to typical practices of children as they go about their daily life and interact with others [17], for example browsing social network profiles, instant messaging, and phone and video conversations [16]. *Geeking out* refers to interest driven participation centering upon specific activities, interests, or niche and marginalized identities [17]. It involves intense commitment with media or technology, often with one particular media property, genre or a type of technology [16], e.g. intense gaming or media production, long term video and music file sharing or engaging in interest groups [16]. Finally, *messing around* describes media engagement in which kids are tinkering, learning, and getting serious about something, often supported by the social networks developed in their friendship- or interest-driven groups. [17]. It is also a transition zone between geeking out and hanging out, and between interest-driven and friendship-driven participation [17], including e.g. using search words/engines to find information about interesting issues, and experimenting with media for example by using photo and video editing tools [16].

No matter whether hanging out, geeking out, or messing around, presence in social media is getting more and more important among children: for instance in Finland the use of social media was mentioned to be the most important use of the Internet for girls aged as young as 10-12, for the boys same age it was trumped only by watching video clips and gaming [37]. The favorite social media of Finnish teens and preteens include Facebook, YouTube, Instagram, Ask FM and Pinterest - gaming platforms like Habbo and World of Warcraft are also familiar [30]. Wikipedia is used in schoolwork [30] and a new favorite is mobile online messaging app "WhatsApp" [30]. In 2010, 67% of Finnish children who used the Internet had their own social networking profile, including 46% of 9-12 year olds, despite the fact that most use Facebook, where the minimum age is 13 [9]. In a national media barometer conducted a couple of years later, it was found that 82% of Finnish children aged 10-12 had a social networking profile [37].

It is a notable development that even if absorption in online communication, i.e. social networking and use of smart phones and video sharing sites have been seen as typical for teenagers [18], it is becoming characteristic of ever younger children [26]. Current research reveals that there has been an increase in Internet usage by children under nine years old [15], [40]. 19% of Finnish children aged 0-3 use the Internet in some way, and between the ages 4-6 the percentage increases to 58% [10]. In addition to watching videos, gaming and doing homework these young Internet users are socializing in virtual worlds meant for children, or as underage participants in social media meant for teenagers and adults [15]. This is a problem as it has not been established that young children have the capacity to engage with the Internet in a safe manner, especially when it comes to social media [15]. The presence of young children in social media can be risky especially concerning contact requests, the publicity of friend network, and the visibility of personal information [21].

4 What do we fear when children are online?

Societal and parental fears over children are not new, but Internet and different technologies have brought additional things to worry about. Some are unique to the Internet, but many can be seen as reformulation or extension to offline threats. [4]

Next, existing research on the threats associated with children's Internet activities is reviewed. In addition to the traditional online threats to information security, children can also encounter threats to their personal safety online. A threat is something that can (intentionally or accidentally) exploit some vulnerability and cause some harm in the process, while risk is a calculation based on probability and the likely consequences of harm, when exposed to a threat [26]. Harm is a distinct and negative outcome, whether measured objectively or, more usually, through subjective self-report [26]. For example, there is a risk that when positioned as a recipient of some inappropriate content [26], children might experience psychological harm [4], or when a child participates in certain online interactions [26], they might experience physical harm [4]. Personal safety is defined as an individual's ability to go about their everyday life free from threats or fear of psychological, emotional or physical harm [42]. Online threats to personal safety can include for example cyberbullying, online predators, and exposure to offensive content.

The threats usually associated with use of mobile technology and Internet have been subdivided into content threats and contact threats [4]. However, also conduct threats [4] and computer/Internet threats [28] can be included in the categorization. *Content threats* include inappropriate content for children, such as commercial spam and targeted emails/ads (treating children as active consumers, unwanted pop-ups) as well as adult/abusive content such as pornography, violence, pro-anorexia and drug related content [28]. *Contact threats* include grooming (adult forming an emotional bond with a child for the purpose of sexual abuse), sexting (sending sexually explicit messages via text or chat), cyberbullying and cyberstalking (using IT to harass someone), and privacy loss [28]. *Conduct threats* include a child being engaged in activities such as illegal file sharing or bullying others [4]. Finally, *Computer/Internet threats* include information security threats like malware (software used to damage a system, to gain access to computers, to gather sensitive information)**,** phishing (trying to get the user to reveal private information by impersonating a trustworthy entity), data theft/loss, password stealing/cracking, and also Internet addiction [28].

The most common risk among Finnish 9-16 year olds is communicating online with persons they have never met offline. Most of these online acquaintances might be friends of friends or friends of family, but children did acknowledge that strangers are a risk. When asked if they have had contact with these persons, previously unknown to them, also offline, 6% of the Finnish children answered they have. "Stranger danger" is one of the most talked about concerns today, even if the danger of actual harm seems to be relatively low – most likely because the possible harm would be so severe. It should be noted, however, that contact with strangers is an integral part of many Internet activities, like gaming, social media, and publishing online. Children are creating a relationship towards the Internet audience, and they are using the Internet to maintain and expand their social contacts. [21]

Children are usually considered to be passively involved in most online threats (for example nobody specifically invites suspicious emails or wants to get bullied or

stalked), however, they do actively participate in the leakage of their own personal information online [28], for example when using social media. If children are not aware of the risks associated to the inappropriate use of their personal and sensitive data, they are vulnerable not only to privacy loss and other contact threats, but also to content and information security related threats [28]. If they share their email address freely, they are easier to approach by online predators, but could also start receiving spam email, links containing viruses and so on. Just over half of European 11-12-year-olds, rising to over three-quarters of the 15-16-year-olds, know how to change the privacy settings on their profile [12]. Most Finnish children have their profile set to private or partially private so that most things they post is only visible to their friends, but 28% still have a public profile [9]. Younger children are more likely to have a public profile, however, they are slightly less likely to disclose their address, telephone number or the name of their school on their profile [12].

On the other hand, it is also important to remember that just because there is a risk that something bad might happen, it does not mean it actually will: most European 9-16 year old children have not been bothered by something experienced on the Internet. Seeing sexual images and receiving sexual messages online is relatively common, but generally not experienced as very harmful. By contrast, being bullied online is relatively uncommon, but it more likely to upset children. It should also be remembered that more use facilitates more digital literacy and safety skills and European pre-teens and teens are generally not unskilled when it comes to online safety: most 11-16 year olds said that they can block messages from people they do not want to contact, and that they can find safety advice online. Around half of them said that they can change the privacy settings of their social media, block websites, and judge the quality of a website. The younger respondents, however, tend to lack skills and confidence. [24]

5 What has been done to keep children safe?

The fast adoption of the Internet and different online technologies presents policy makers, governments, and the industry the tasks of identifying the threats and risks of Internet use and developing strategies and tools to make sure that harm linked with them is minimized [33]. In a more grass-root level, parents, schools, and even other children are involved in a more practical way in seeking to maximize online opportunities while minimizing the possibility of harm [12]. Next, a variety of mechanisms aiming at protecting children's online information security and personal safety are identified from the existing literature.

5.1 Industry mediation

Most social media are intended for teenagers and adults. Age limit to use for example Facebook, Tumblr, Instagram, ask.fm, YouTube and Google+ is 13. Some social media are however clearly targeted for children, such as Momio, Club penguin and Habbo hotel. However, service providers rely on users' self-professed age [3]. Although the industry providers try to limit their services for appropriate users only, in the Internet no-one still knows if you're are as young or old as you say you are.

Moreover, the services have different privacy policies and settings available for their users, but the settings have been criticized for having too weak defaults for their younger users [15] and the privacy policies for being generally vague or non-transparent [1].

Additionally, the industry applies different mechanisms to screen off offensive content, using e.g. keyword blacklists or offering users possibility to report offensive content. However, most social media use a simple lexicon-based automatic filtering approach that is not very accurate and might generate many false positive alerts [38]. In addition, when these systems depend on users and administrators to detect and report offensive contents, they might fail to take quick actions. For children who often lack cognitive awareness of risks, these approaches are not effective either [38].

5.2 Technical mediation

In addition to protecting the computer itself from e.g. viruses, different solutions for technical mediation are available for parents, such as software for filtering and restricting unwanted use. Three quarters of parents adopt technical mediation through the use of parental control or some other means of blocking and filtering certain types of websites. [12]

Criticism against these kind of software include, e.g., that they are not as good in blocking non-English language content, and that there is a tradeoff between underblocking (permitting sites that should be blocked) and overblocking (blocking sites that should be permitted). There are also some ethical considerations: although law might give the parents grounds to monitor their children online to keep them safe it should still be asked if full-scale monitoring of children is ethically acceptable. [28]

5.3 Social mediation

Today, children's use of Internet and mobile technology is becoming more private and inaccessible to parental oversight [23], thus making monitoring of children's online activities harder. Parents are often caught in the middle, wanting their children to fit in and to widen their social circles, but at the same time knowing that most social media were not designed for children [25]. However, parents are encouraged to take measures to protect their children from risks; proactively engaged parents are seen as "good" parents [4]. Making sure that children are safe is a combination of protecting children and giving them tools to cope with the potentially harmful things they encounter, but also making sure that they are not making wrong decisions that might have severe consequences [45].

Different kinds of strategies can be employed for reducing the risks that children face online, e.g. active mediation of children's Internet use (talking to them and offering help), restricting the use, or monitoring it (checking the computer, profiles on a social networking site or messages etc.). Nine out of ten European 9-16 year olds tell that their **parents** advise them about Internet use and Internet safety, and they have restrictive rules at home, whereas monitoring is only experienced by half of the children. Parents are the main mediators about safety. However, the role of **teachers** is also important; especially for children from lower income homes. This should lead

public policies to more information campaigns targeted at teachers. Teachers mostly practice restrictive mediation: over 60% of European children say that their teachers set rules for using Internet at school. Only one-quarter say their teachers have helped when something bothered them on the Internet, but this can reflect to the fact that relatively few incidents bother children. However, one in five children report that their teachers have not engaged with them at all. On the other hand, **peers** play a major role when seeking social support: children turn to them first, whatever the problem. Three-quarters of children say their peers have helped or supported their Internet use in practical matters but not as often when they are bothered by something, but as noted before regarding teachers, this may reflect the fact that few are bothered. [12]

Children do want to talk to someone about their experiences online [32], and addition to viewing children's online safety as something that depends on others, it can also be seen as an action by children enabled by their growing independence and as a developmental process [45]. Their skills related to online behavior also develop differently [39] and their developing moral judgment skills affect their behavior [45].

5.4 Policies and educational efforts

There are diverse and motivated efforts underway in many countries to promote digital learning technologies in schools, e-governance initiatives, digital participation, and digital literacy [33]. These include initiatives on e.g. European Union level, such as The Safer Internet Programme and European Strategy for a Better Internet for Children. The associated Safer Social Networking principles for the EU have been signed by most of the industry providers in Europe. The aim of the program is to give children the skills and tools they need to safely benefit from being online. To do this, the European Commission is seeking to identify how national education systems approach online safety issues and what children learn about online safety in school [7].

In Finland, topics related to online safety are included at schools in subjects related to the development of media and communication skills [7], [39]. Educational efforts are also made by national actors such as the Mannerheim League for Child Welfare, National Audiovisual Institute, Save the Children Finland, and Finland's national public service broadcasting company. There are also countless educational efforts made by researchers and other interested parties, for example different guidebooks for children [29], [44], guidebooks for parents [6], [43], and a prototype of an educational information security board game [36]. However, educating children about these issues can be problematic, especially if children feel that they are more competent technology users than their instructors [36]. This likely will not be a problem in Finland in schools or at home as Finnish children have acknowledged that in fact their parents are more competent media users than they are [30]. Moreover, we often erroneously presume a gap between educators and students. If such a gap does exist, it is definitely possible to close it by acquiring skills and experience in interacting with ICT [14].

6 Research Contributions and Gaps

The field of online safety is increasingly attracting scholarly interest from various disciplines ranging from psychology to IS. This study aimed to produce an understanding of the state-of-the-art of multidisciplinary research on children's online safety for the IS researchers to enter into. This was quite a complicated task as research on the topic forms a diverse and relatively new field without widely accepted theoretical frameworks or standard methodologies, and where definitional, measurement and interpretative challenges prevail [26]. The review was accomplished by reviewing research on children's online activities, threats and risks associated with it and different initiatives taken to secure children online. Figure 1 summarizes the main findings of the literature review.

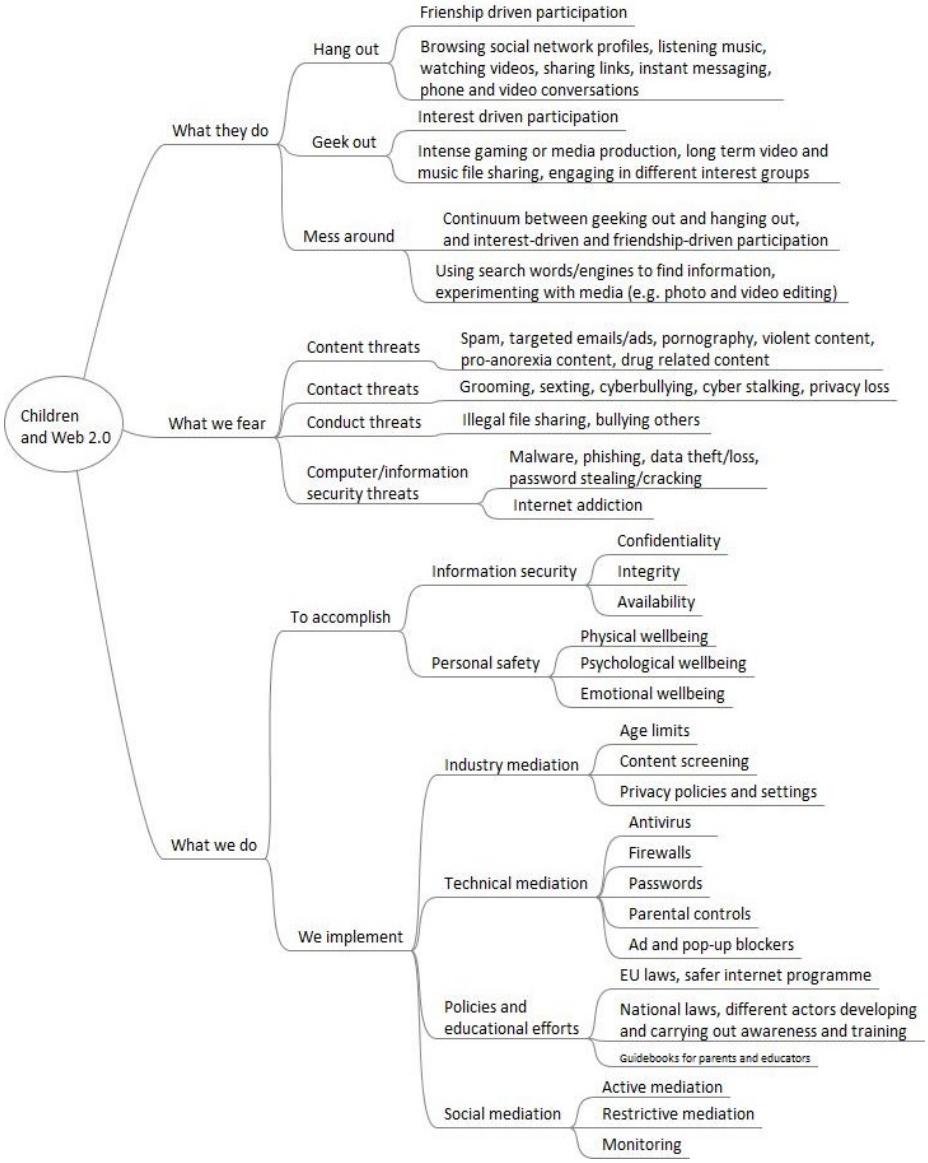

Fig. 1. Children online: What they do, what we fear, what is done to make them safe

Children engage online in a variety of activities, characterized as *hanging out*, *geeking out* and *messing around*, and presence in social media is getting more and more important (Fig. 1). There has been a substantial increase in Internet usage by very young children, whose presence in social media can be risky in many respects.

The threats associated with Internet use have been divided into *content threats*, *contact threats*, *conduct threats*, and *computer/Internet threats*. Most European teens

and preteens are quite skilled in online safety, however the younger the children, the more likely they lack skills and confidence.

Luckily, however, there are many actors and efforts involved in trying to make children safe online. To accomplish *information security* and *personal safety* of children *industry mediation* offers privacy policies and settings in services and enforces age limits, as well as applies mechanisms to screen off offensive content, while they are not very accurate and might generate many false positive alerts. *Technical mediation* can be employed, while criticism against software for filtering and restricting has also been expressed. Moreover, there are ethical considerations related to this. Different *policies and educational efforts*, on the other hand, include diverse efforts to promote digital learning in schools, different e-governance initiatives, digital participation, and digital literacy and online safety. As regards *social mediation*, different kinds of strategies can be employed e.g. active mediation of child's Internet use, restricting the use or monitoring it. Parents are the main agents here; however, the role of teachers and peers also appears as important.

A number of research gaps were also identified during the literature review, related to which also IS researchers could contribute. Those are listed in Figure 2.

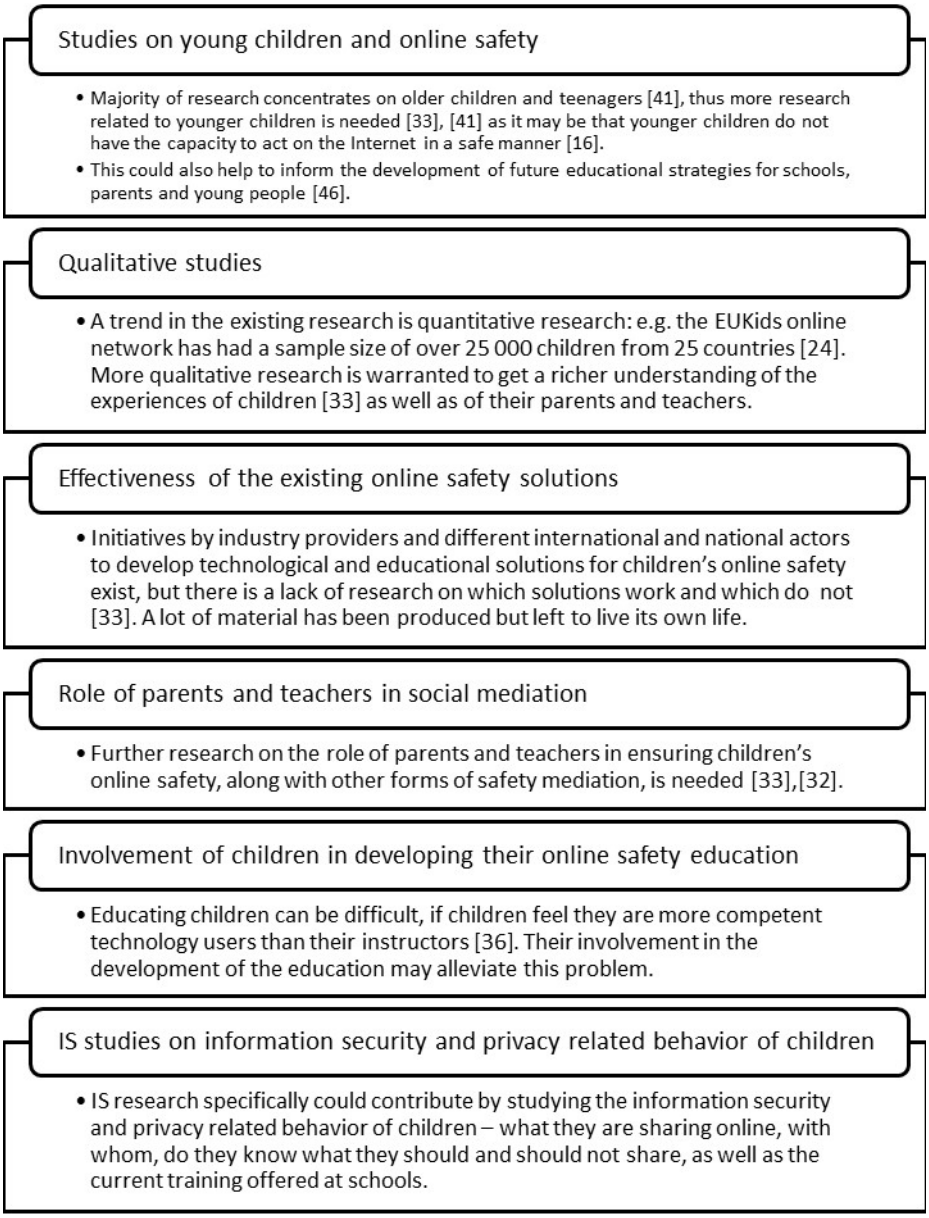

Fig. 2. Research gaps and their explanations

While personal safety is buzzing and much researched topic by psychologists, sociologists and pedagogy professionals, there seems to be room for information security related research concerning children and their online activities. The topic should not be avoided by IS researchers: instead of assessing the risk of harm to

firewalls or corporate assets, the focus here is in the risk of harm to a much more precious entity – the child. It is true that research on online risky behavior and possible harm to children is perhaps best left to someone more equipped to assess psychological factors, but IS research could also clearly contribute to this new, extremely important and highly fascinating topic of study.

7 Conclusions

This study aimed to produce an understanding of the state-of-the-art of multidisciplinary research on children's online safety for the IS researchers to enter into. This was accomplished by reviewing the current body of knowledge concerning children's online activities, and related threats and risks, as well as initiatives to achieve online safety. Large amount of research originates from disciplines such as psychology, sociology, and media studies. The buzz seems to be mostly on the personal safety side – scholars are investigating what kinds of risks children take, and what kind of threats they are facing. Even though there is much research on the IS side about the Internet and information security, it tends to focus on adults, and organizational or technical aspects. Worthy topic, in addition to securing corporate reputation and assets, would be for the IS community to help securing the future – the children. At this moment research originating from the IS community concerning this topic is scarce, even though good information security lays the groundwork for privacy, which in turn is the cornerstone for children's online safety. IS researchers could contribute to this area greatly for example by studying information security and privacy related behavior of children, and different available trainings and their effectiveness.

8 References

1. Anthonysamy, P., Greenwood, P., Rashid, A.: Social Networking Privacy: Understanding the Disconnect from Policy to Controls. Computer, 46 (2013) 60-67
2. Boell, S. K., & Cecez-Kecmanovic, D.: On being `systematic' in Literature Reviews in IS. Journal of Information Technology, (2014) 1-13
3. boyd, d., & Hargittai, E.: Facebook Privacy Settings: Who Cares? First Monday, 15 (2010)
4. boyd, d., & Hargittai, E.: Connected and Concerned: Variation in Parents' Online Safety Concerns. Policy & Internet, 5 (2013) 245-269
5. Cronin, P., Ryan, F., Coughlan, M.: Undertaking a Literature Review: A Step-by-Step Approach. Br. J. Nurs., 17 (2008) 38-43
6. Edgington, S. M.: The parent's guide to texting, facebook, and social media: Understanding the benefits and dangers of parenting in a digital world. Brown Books Publishing Group (2011)
7. Eurydice network: Summary Report: Education on Online Safety in Schools in Europe. (2010) 20
8. Gross, R., & Acquisti, A.: Information Revelation and Privacy in Online Social Networks. (2005) 71-80
9. Haddon, L., & Livingstone, S.: EU Kids Online: National Perspectives. (2012) 74

10. Happo, H.: Lapsiperheiden mediakysely 2012: 0-12 vuotiaiden lasten internetin käyttö ja mediakasvatus kotiympäristössä. In: Kupiainen, R., Kotilainen, S., Nikunen, K., et al (eds.) Lapset netissä: Puheenvuoroja lasten ja nuorten netin käytöstä ja riskeistä, pp. 25-36. Mediakasvatusseura, Helsinki (2013)
11. Harris, S.: Cissp certification exam guide. Osborne/McGraw-Hill (2002)
12. Hasebrink, U., Görzig, A., Haddon, L. et al.: Patterns of Risk and Safety Online: In-Depth Analyses from the EU Kids Online Survey of 9- to 16-Year-Olds and their Parents in 25 European Countries. (2011) 87
13. Hekkala, R., Väyrynen, K., Wiander, T.: Information Security Challenges of Social Media for Companies. ECIS 2012 Proceedings, (2012)
14. Helsper, E. J., & Eynon, R.: Digital Natives: Where is the Evidence? British Educational Research Journal, 36 (2010) 503-520
15. Holloway, D., Green, L., Livingstone, S.: Zero to Eight. Young Children and their Internet Use. (2013) 36
16. Horst, H. A., Herr-Stephenson, R., Robinson, L.: Media ecologies. In: Ito, M. (ed.) Hanging out, Messing around and Geeking out: Kids living and learning with new media, pp. 29-78. MIT Press, Cambridge (2010)
17. Horst, H. A., Herr-Stephenson, R., Robinson, L.: Media Ecologies, Genres of Participation. (2008) spotlight.macfound.org/blog/entry/horst-herr-robinson-media-ecologies/
18. Ito, M., Horst, H. A., Antin, J. et al.: Hanging out, messing around, and geeking out: Kids living and learning with new media. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. MIT Press (2010)
19. Kaplan, A. M., & Haenlein, M.: Users of the World, Unite! the Challenges and Opportunities of Social Media. Bus. Horiz., 53 (2010) 59-68
20. Kietzmann, J. H., Hermkens, K., McCarthy, I. P. et al.: Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media. Bus. Horiz., 54 (2011) 241-251
21. Kupiainen, R.: EU Kids Online: Suomalaislasten netin käyttö, riskit ja mahdollisuudet. In: Kupiainen, R., Kotilainen, S., Nikunen, K., et al (eds.) Lapset netissä: Puheenvuoroja lasten ja nuorten netin käytöstä ja riskeistä, pp. 6-15. Mediakasvatusseura, Helsinki (2013)
22. Lietsala, K., & Sirkkunen, E.: Social media. Introduction to the tools and processes of participatory economy. Hypermedia Laboratory Net Series. 17th edn. University of Tampere, Tampere, Finland (2008)
23. Livingstone, S.: Children and the internet. Polity (2009)
24. Livingstone, S., Haddon, L., Görzig, A. et al.: Risks and Safety on the Internet: The Perspective of European Children. Full Findings. (2011)
25. Livingstone, S., Ólafsson, K., Staksrud, E.: Risky Social Networking Practices among 'Underage' Users: Lessons for Evidence-Based Policy. J Comput Mediat Commun, 18 (2013) 303-320
26. Livingstone, S., & Smith, P. K.: Annual 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. J. Child Psychol. Psychiatry, 55 (2014) 635-654
27. Lucas, M. M., & Borisov, N.: flyByNight: Mitigating the Privacy Risks of Social Networking. WPES '08, (2008) 1
28. Magkos, E., Kleisiari, E., Chanias, P. et al.: Parental Control and Children's Internet Safety: The Good, the Bad and the Ugly. ICIL, (2014) 18
29. Minton, E.: Social networking and social media safety. Stay Safe Online. Powerkids Pr (2014)

30. Noppari, E.: Mobiilimuksut. lasten ja nuorten mediaympäristön muutos, osa 3. Tampereen Yliopisto, Tampere, Finland (2014)
31. Nosko, A., Wood, E., Molema, S.: All about Me: Disclosure in Online Social Networking Profiles: The Case of FACEBOOK. Comput Hum Behav, 26 (2010) 406-418
32. Oinas-Kukkonen, H., & Kurki, H.: Internet through the Eyes of 11-Year Old Children: First-Hand Experiences from the Technological Environment the Children Live In. Human Technology: An Interdisciplinary Journal of Humans in ICT Environments, 5 (2009) 146-162
33. Ólafsson, K., Livingstone, S., Haddon, L.: Children's use of online technologies in europe: A review of the european evidence base. EU Kids Online, LSE, London (2013)
34. Prensky, M.: Digital Natives, Digital Immigrants Part 1. On the Horizon, 9 (2001) 1-6
35. Prensky, M.: Digital Natives, Digital Immigrants, Part II: Do they really Think Differently? On the Horizon, 9 (2001)
36. Reid, R., & Van Niekerk, J.: Snakes and Ladders for Digital Natives: Information Security Education for the Youth. Information Management & Computer Security, 22 (2014) 179-190
37. Suoninen, A.: Lasten mediabarometri 2012: 10-12 vuotiaiden tyttöjen ja poikien mediankäyttö. Verkkojulkaisuja, Vol. 62. Nuorisotutkimusverkosto, Helsinki, Finland (2013)
38. Tomer, P., Lade, S., Kumar, M. S. et al.: On Line Social Network Content and Image Filtering, Classifications. IJERST, 2 (2013) 16
39. Tuominen, S.: Toiminnallisuutta nettikasvatukseen. In: Kupiainen, R., Kotilainen, S., Nikunen, K., et al (eds.) Lapset netissä - Puheenvuoroja lasten ja nuorten netin käytöstä ja riskeistä, pp. 92-100. Mediakasvatusseura, Helsinki, Finland. (2013)
40. Walamies, T.: Poimintoja 0-8-vuotiaiden mediasuhteita koskevasta tutkimuksesta. In: Kotilainen, S. (ed.) Mediabarometri 2010: 0-8 vuotiaiden lasten mediankäyttö Suomessa, pp. 9-14. Mediakasvatusseura ry, Helsinki, Finland. (2011)
41. Wallace, P.: Information systems in organizations. Prentice Hall (2013)
42. Waters, J., Neale, R., Hutson, S. et al.: Personal Safety on University Campuses - Defining Personal Safety using the Delphi Method. 20th Annual ARCOM Conference, 1 (2004) 411-418
43. Whitby, P.: Is your child safe online? A parent's guide to the internet, Facebook, mobile phones & other new media. White Ladder Press (2011)
44. Willard, N. E.: Cyber savvy: Embracing digital safety and civility. Corwin (2011)
45. Wisniewski, P. J., Xu, H., Rosson, M. B. et al.: Adolescent Online Safety: The "Moral" of the Story. Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing, (2014) 1258-1271