Cyber Security Risks for Minors: A Taxonomy and a Software Architecture

Andreas Tsirtsis*, Nicolas Tsapatsoulis*, Makis Stamatelatos‡, Kwstantinos Papadamou† and Michael Sirivianos†
*Dept. of Communication and Internet Studies
Cyprus University of Technology, CY-3036, Limassol, Cyprus
e-mail: andtsirtsis@gmail.com, nicolas.tsapatsoulis@cut.ac.cy
†Innovators S.A., Antheon 1, Alimos 174 56, Greece
e-mail: m.stamatelatos@innovators.gr
‡Dept. of Electrical and Computer Engineering
Cyprus University of Technology, CY-3036, Limassol, Cyprus
e-mail: ck.papadamou@edu.cut.ac.cy, michael.sirivianos@cut.ac.cy

***Abstract*—The explosion of the Internet provides a variety possibilities for communication, finding information and many other activities, turning into an essential tool in our modern everyday life. However, its huge expansion globally has created some serious safety issues, which require a special approach. One of these issues and perhaps the most important one concerns the safety of children on the Internet, as they are more exposed to dangers and threats in comparison with adults. In order to design effective measures against these threats and dangers deep understanding of minors' activities on the Internet, along with their motivation, is a first necessary step. It is shown in this report that minors' Internet activity tends heavily, and in an increasing manner, towards Online Social Networks (OSN). Thus, Internet filtering techniques designed and applied so far for child online protection need to be reconsidered and redesigned in a smarter way such as data analytics, advanced content analysis and data mining techniques are incorporated. OSN fake account identification, sexual content detection and flagging of multiple OSN accounts of the same person are examples that require such sophisticated techniques. This study deals with a literature review concerning the Internet activity and motivation of use by minors and presents in a coherent manner the identified risks and threats that children using the web and online social networks are exposed to. It also presents a systematic process for designing and developing modern and state of the art techniques to prevent minors' exposure to those risks and dangers.**

***Index Terms*—cybersecurity risks, online threats, minors, privacy, online social networks, taxonomy**

I. Introduction

The rate at which families gain access to the Internet is constantly increasing. According to ITU's "Measuring the Information Society Report" 1.5 billion people had access to the Internet in 2009 with this percentage peaking at 3.5 billion in 2015 [1]. Unfortunately, access to the Internet raise also serious safety issues which have to dealt with especially when it comes to minors. One of the most important steps is awareness of what children actually do while being online.

It is important to define what is meant by the term minors. Minors or youth refers to individuals who are younger than 18 years of age. The term children refers to minors whose age ranges between 0-12 years old, while the term adolescents or teenagers is used to describe minors between 13 -17 years old. The difference between these age categories is crucial as the possibilities, way of thinking, and the activities and needs of children change. For this reason, ITU (International Telecommunication Union) has categorized the rules and guidelines dividing them into five categories depending on children age, broadly corresponding to the key stages of development of a child's growth to adulthood [2].

The first category includes children aged to 2-4 years old. The children in this category have not yet developed critical thinking so that they can use the internet on their own. Furthermore, whatever they look at is received by them at face value [3]. The second category concerns children aged between 5-7 years old. At this age children have not developed critical thinking as well as on the first category and they also accept whatever they see at face value. The difference however, at this age they are able to use computers or smartphones in order to play games. This can make then vulnerable to online marketers who ask for personal information through surveys or filling registration forms.

The third category refers to children aged 8-10. At this age children are able to communicate with people will do not really know. They are interested in older children activities and get pleasure by playing games and surfing the internet. In addition they may be using an email with which they have may contact with others either through chat rooms or social networks [4].

The fourth category includes children aged 11-13 years old. At this age children are most vulnerable to become victims of sexual predators. They may be using the Internet for help with some school assignments, to search difference sites, to communicate or to download content. Children at this age range are sensitive as far as sexual development is concerned and may attempt to access pornographic sites - especially the males [5], [6]. The fifth category concerns children aged 14-18. Children at these ages have access to almost all possibilities that Internet provides. They are interested in developing online relationships and may have some real life meeting as well.

978-1-5090-5246-2/16/$31.00

Furthermore, they may use social media so as to contact adults. At this age range children are more prone to receive any sexual comments online [7].

II. Minors' access to the Internet and use of Online Social Networks (OSN)

Nowadays, children are very familiar with technology. Research has shown that they have the ability to familiarize themselves with any electronic gadget very fast and they are able to do sophisticated tasks using these devices. Research has also proven that as soon as children come in touch with electronic device such as PC's, tablets, smartphones and so on, they can use them instantly, in contrast with adults who may need to study the instructor manual of the gadget.

More and more children, these days, have access to the internet through handheld electronic devices such as smartphones, tablets and portable game consoles [2]. According to Ofcom reports on Internet safety measures and strategies of parental protection for children online in the UK [8], [9] tablets became the favorite device for online access for children aged 8-11 who mostly used them for playing games. Smartphones are the most popular device for social networking and, according to the same reports, the children aged 12-15 have their own smartphone. Most parents believe that children are more at risk when they are online at home than outdoors. However, statistics have proven the opposite. This is because smartphones, tablets and other handheld devices, offer instant access to the Internet everywhere and children prefer that as they are not supervised by their parents. According to the 2016 ITU report on child online protection in USA [2] the number of children who have access to the internet is constantly increasing since 2011. Children below five years of age use the internet on a weekly basis and as age increases the frequency of access to the internet also increases. The 40% of children aged 8-11 years old make use of the internet daily while the 36% of them use it multiple times per day. The same report reveals that 70% of teenagers are online daily while 25% of them reported that they are permanently connected online. A survey conducted by South Korean government [10] has shown that one out of ten children aged 10-19 years are addicted to the Internet. According to that study, when children are connected online they enjoy using a variety of activities whose number increase by age. For instance, children under 9 years old search for information about school, play games or watch videos (see also [11]). Children aged 10 to 19 also listen to music as well as the above mentioned activities, however their basic everyday use of the internet is for social networking reasons.

The intrusion of online social networks in people's everyday life the last decade, has met with huge success. There are many social networks services available, so as to meet different needs according to age, language, profession and culture. According to the 'Net Children Go Mobile' network report [12], approximately 70% of children in Europe have at least one social network profile while most of them have a profile in media sharing services such as YouTube or Instagram. In UK one out of four children use Twitter to share photos and other content [13] rather than tweeting. A study conducted by Pew Research Center for USA [11] colcluded at similar findings. Facebook is the most popular social media site among American teenagers aged 13 to 17 since 71% of them are using the corresponding website. Half of teens use Instagram, while the popularity of Snapchat increases rapidly reaching a 41% of teens population. Snapchat allows people to send and receive pictures and videos directly to their phone and created new security concerns for parents [14]. The study of Pew Research Center showed also that about 71% of teens are using more than one online social network site [11].

III. A taxonomy of online risks for minors

It has being shown in the previous section that the popularity of Internet in general and OSN in particular is high and with increasing tendency among children and teenagers. Thus, the online risks for for these sensitive age categories received increased awareness. Several different international organizations and research groups have been trying to study and categorized the dangers which have emerged in the past years including EU Kids Online[1], ITUs-Child Online Protection (COP)[2], Youth Protection Roundtable (YPRT)[3], Net Children Go Mobile[4] and many others. These organizations conduct surveys in regular time intervals and, based on the findings, recommend safety measures for every identified potential danger that the Internet might pose to children. However, the security and privacy risks themselves are rarely mentioned making it difficult to define energetic actions and to design tools that proactively try to minimize the aforementioned risks and dangers. For instance, in contrary to a few studies such as those of Australian Communications and Media Authority [15], [16] where dangers, of Internet and OSN use, such as electronic fraud, malware and other e-safety threats, are explicitly mentioned, research in Europe usually describes generic categories of risks such as sexual and commercial.

Categorization of online risk for children is not easy. In most cases risks are caused or affected by a variety of reasons emanating not only from children's online lives but their real lives as well. In addition many risks and threats are crossing several categories. In the corresponding literature the following distinctive situations have been defined [2], [13], [17]:

- Online risks which are the expansion of problems in real life, for example pornography.
- Risks which arise from the interaction of two under-agers such as cyberbullying.
- Risks which arise from the interaction between a child and an adult, such as cyber grooming.
- Risks which arise by the collection of data, against the protection of privacy, such as viruses and other malware.

In addition of potential dangers, children on the internet might be exposed to, can be assessed based on the legal

[1] www.eukidsonline.net
[2] http://www.itu.int/en/cop
[3] http://www.yprt.eu/yprt/content/sections/index.cfm/secid.90
[4] http://netchildrengomobile.eu

TABLE I
CHILDREN'S MAIN ONLINE ACTIVITIES AND ENCOUNTERED DANGERS AND RISKS PER AGE CATEGORY

Age range	Popular online activities	Main dangers and risks
1-4	music listening and videos watching, random access to websites	whatever they look at is received at face value
5-7	use computers or smartphones in order to play games	victims of online marketers, personal information leaks
8-10	online gaming, surfing, chatting	they can contact older (unknown) children and/or adults
11-13	Web search, online games, chatting, use of e-mail, use of OSN	victims of sexual predators, illegal content, cyberbulling
15-18	extensive use of OSN, any Internet activity	recipients and senders of sexual content, cyber grooming

importance and by discriminating the cases where the child is the victim or the predator.

Another popular, in the related bibliography, categorization of online risks is based on the way the Internet is 'used' and/or perceived by the children. The first clearly concerns the risks of the Internet as product of technology or simply stated the risks that arise due to minors' access to Internet content. The second category, concerns incidences where the Internet provides the means through which the children are exposed to dangers, i.e., contact risks, and finally, the third category refers to cases where children are aimed at as online consumers [18], [19].

A. Content risks

As already stated, children are able to familiarized themselves with Internet and generally with technology as they grow up parallel to it. This fact combined with the fact that in 2015 there were more than one trillion websites, turns children into a vulnerable group or exposed to many dangers related to the content of the Web. Content risks can roughly divided in three categories: (a) illegal content, (b) harmful content or age inappropriate content and (c) harmful advice.

Illegal content refers to content which is illegal to be published online. For example, it might be content about sexual exploitation of children which is illegal in most countries. Inappropriate content usually depends on the age of children that have access to and may contain, for instance, adult pornography. Hatred or violence related content, although not illegal, may harm children in case they gain access to it. Age inappropriate content may be mentioned, as term in national or local cultures and social values, however, in literature and official documents [19] this term focuses more widely on pornography and other sexual content. The meaning of pornography may vary between countries and between groups within a country. Pornographic content is fairly easy to be found by anyone online, however, according to a 2008 study [20], younger children are more exposed to offline pornography than online ones. Nevertheless, a lot of studies agree that exposure of children to online pornography content increases by age. In addition it was found that random exposure of children to pornographic content, on the Internet, is more common than intentional access and it increases when the names of the websites or URLs are misleading for children. According to ITU [2] the rates at which children of young ages are exposed to websites of pornographic content appears an increasing tendency. This happens even to children whose parents have locked access to sites of inappropriate content. The high percentage of children that randomly access to pornographic content continues with intentional access . According to Dooley *et al*. [21] only children of very early age reported being upset by being exposed to pornographic content. As for the exposure of children to violate content researchers did not arrive yet at concrete findings and it seems that additional research is required.

Harmful advice refers to content which may lead a child to consume alcohol and drugs or to commit suicide or different psychological and nutritional disorders. In combination with the fact that anyone can provide such advice online through social networks and other platforms, it is very easy to children to have access to and be influenced by it. Researchers state that many of these advices maybe well intended; thus, it is difficult to be categorized to harmful or useful [19].

B. Contact risks

Contact risks refer to instances or events that children have direct interaction online, either with other children or with adults. This can be achieved through child's participation in online chat or social networks chats. A frequent phenomenon is when adults try to develop relationships of trust with children with the aim of having sexual intercourse with them. This constitutes a criminal act in almost all countries and is known as cyber grooming [19], [2]. Cyber grooming is often when an adult sexual predator seeks a communication with its victims in a direct online conversation with the aim of coming in offline sexual relation with them without mentioning his/her real age and identity to the children taking advantage of their naivety [22].

Cyberbulling is another contact risk for the children. The term refers to bullying that children undergo through the Internet. Bullying may come in different types such as threats, humiliation or harassment. Cyberbullying differs from cyber stalking and cyber harassment. While in cyberbullying there is participation of peers of both sides, in the event of an adult participant it constitutes cyber harassment [23]. According to studies, the reason why the phenomenon bullying on the internet manifest are many. Experiencing tense emotions such as anger, desperation or vengeance are frequent reasons causing children to be exposed to cyberbullying. Emotions which stem from problematic situation in the family background and problematic relationships in general are also common reasons. Researchers indicated that cyberbullying constitutes in many

cases some form of entertainment, satisfying in this way power struggle needs.

In comparison with traditional bullying, cyberbullying offers some advantages to predators. The most important of which is the ability to remain anonymous which they achieve by using aliases, fake profiles, fake accounts, face social media profiles, text messages, instant messaging and other services that internet provides so they do not reveal their identity. Cyberbullying is one of the biggest threats that social networks pose. In recent years more than three million children have undergone cyberbullying in any form whether this constitutes harassment or threats; a high percentage (95%) reported that they have been victims of cyberbullying on Facebook.

Eight out of 10 adolescents who use social networks share personal information about themselves such as photos or videos, location information and contact information to a much greater extent compared to previous years. According to several studies [20], [24] sharing personal information such as age, phone number, school and location are the main reasons for young people to undergo cyberbullying through social networks. In recent years electronic games have shown an enormous increase. These games either through PCs or game consoles support features for online games and games with multiple players. Most of them have special chat rooms so that communication among players may be easily achieved. Robinson's research [10] indicates that approximately 20% of the children who reported having undergone some kind of cyberbullying where cited cyberbulling to have being taken place during in an online game. The most usual way of cyberbullying in an online game refers to schools, online game communities and direct communication between online players. OECD [19] reports that the risks that minors run for sexual harassment by adults is limited; 25% of young children share information and interact with strangers on the Internet, however, only 5% of them had spoken to a stranger discussing sexual matters. In addition it is mentioned by OECD that most children tend to ignore the conversation and take proper steps. It is noteworthy that potential sexual predators are adolescences and adults younger than 21 years old. In general, the possibility of physical sexual contact with an adult through an online approach is very rare. Ybarra [25] reports that only eight out of a sample of 1500 hundreds reported physical sexual contact, all of whom where aged 17 and above. Furthermore, it was found [24] cyber grooming for children aged of 12 or less is extremely rare. These results indicate that cyber grooming contains minimum danger, however it is difficult to measure precisely. Research agrees that online harassment constitutes the most widespread Risks that children face. Various individuals use the means of technology offers (social media, chatrooms etc), with a view to harming others through bullying, humiliation and embarrassment and treats. Those who cause cyberbullying are underagers as are their victims. Despite this there have been instances where cyberbullying is caused by adults. Cyber talking refers to the event where an individual is exposed to an online extreme behavior of another individual whose purpose is malevolent treats and/or psychological or physical predicament of the victim. Overall, cyberbullying and cyber harassment constitute an ever increasing field the prevalence of which is extremely worrying [23].

C. Children targeted as consumers

Children on the Internet face the risks of consumers, mostly for products and services designed only for adults. Such cases relate mostly to products such as alcohol, tobacco and prescription medicines. Children may come in contact with advertisements about these products. Commercial marketing messages which may take advantage of their experience, gullibility and curiosity. Furthermore, children may come in contact with the promotional illegal products such as drugs or doping substances. A study in US [26] showed that 75% of teenagers that tried to buy cigarettes online managed to do so, while in 2002 only a percentage smaller that 3% had succeed in doing so.

Minors and more specifically young children are not able to realize that content on the Internet is produced and that is why they have difficulty critically assessing advertisements and advert messages. There have also been instances where online marketing exclusively targets websites for children for example online games. This fact has caused may countries to question integrated ads on websites aimed to children. Online marketing and advertisements may harm children. This happens mainly with products or services aimed for adult such as gambling, pornographic content and dating services. A study by Netchildren [12] show that about 10% of the ads were about games and 5% about dating services. Advertisement of pornographic content from banners and popups constitute the main reason while children accidentialy came in contact with improper content.

D. Economic risks

It is a frequent phenomenon for children to spent exorbitantly if they have access to payment methods either through a mobile phone or other online services, thus creating huge cost for parents [7]. The most usual instances are by registering and transferring money in gambling and other online games. Many games require some form of subscription for some particular reason or to support multiplayers. Players may a spend a lot to buy virtual characters or other features. There are, however, cases where children may spend huge amount of money through fraudulent transactions [20]. This occurs when services do not clarify that after the purchase of a product or service there would be extra charges. A common example of this are ringtone download services for mobile phones who charge extra for registration. According to OECD [19] in 2008 24% of Belgian adolescents reported having paid more for ringtone downloaded and 9% registered in such kind of service without realizing it. All the above risks are exacerbated with children of younger ages because of their inexperience. Nevertheless, minors who do not own a bank account or have access to their payment methods are less likely to suffer economic fraud.

E. Online privacy risks

Safety risks for private life information relate to all users. Children however , constitute an especially vulnerable group as the dont possess the necessary critical thinking to understand and predict the consequences. Personal information privacy in the case of children is at risk where the personal data is collected on the internet automatically following their request to search engines or other services. This may happen in various ways, the most usual is which collecting cookies, electronic registration in surveys and filling information data in electronic forms . In addition children as well as most adults, skip user term in order to have access to services they are interested in. According to OECD [19] 40 websites especially offered for children will analyzed and almost 75 of them ask for personal data. In most websites it was not compulsory however they did ask for personal data such as email age, birthday etc. so that they could gain access to subpages of the site [27]. There are also different websites who target children and the collection of their personal information offering quiz, competitions, research, using marketing techniques, such as a discount or free service or an award managed to gain the personal data as well as their families or friends. The research show that minors give out personal information easier than adults in order to receive an award [26]. Children may share and reveal personal data a because they cannot realize how widespread online viewers are, neither all the possible consequences. Underagers have also addicted social networks and other apps to great extent, publishing information photos videos, thus revealing important information about their life family, friends and of course themselves [22].

IV. An architecture for energetic and proactive protection from security and privacy risks

It should be clear from the previous literature review that guidelines and/or traditional filtering cannot be seen as proactive and energetic means for protection against online security and privacy risks. The majority of these risks are not site or activity dependent but are hidden in the content whether this is text in chatrooms of online games and OSN, photos or videos shared across OSN such us Facebook, Instagram and Snapchat, or simply the content of a web-page. Child online protection needs to be reconsidered and redesigned in a smarter way such as data analytics, advanced content analysis and data mining techniques are incorporated. OSN fake account identification, sexual content detection and flagging of multiple OSN accounts of the same person are examples that require such sophisticated techniques. This study presents the ENCASE high-level architecture (see Figure 1) which is the result of the work of an international consortium[5] composed of top research institutes and companies working in the area of Internet security across Europe.

The ENCASE architecture was designed to safeguard the security and privacy of minors against malicious actors in OSNs having as primary investigation scenarios cyberbullying

[5]http://encase.socialcomputing.eu/

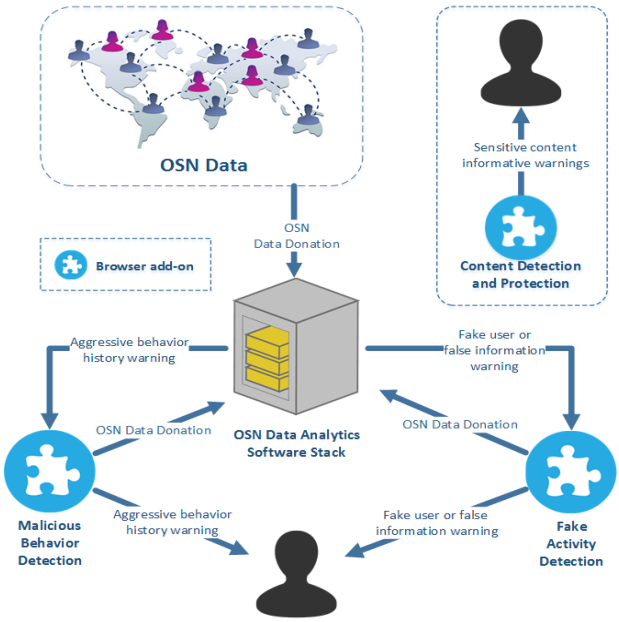

Fig. 1. A high-level architecture for energetic proactive protection from online security and privacy risks.

and online sexual abuse. Both scenarios make use of fake OSN accounts. Existing work on the detection of fake OSN accounts and fake information for OSN platforms, does not address important needs, which include: a) considerations for individual differences regarding online social interactions by minors, e.g., taking into account the particular usability requirements such as accessibility, user engagement, ease of use, error prevention and recovery, and cognitive abilities of users; b) the capacity for early detection of aggressive online users that exploit the open and social nature of these platforms, and the detection of the correspondingly distressed victims; c) the ability to demote the content and communication produced by malicious users that misrepresent their identity and intentions, and to reduce its impact on the legitimate user base; d) the creation of software tools that can be pushed to the interested user base without the need for OSN providers to adopt the architecture from the start of its deployment, i.e., the software suit should rely heavily on browser add-ons; e) the ability to efficiently perform computations over rapidly growing data records of user activity using massively parallel computations tailored to online social workloads.

Techniques integrated through the ENCASE architecture include:

- Large scale analysis of OSN information, such as graph analysis and time-dependent social web data mining, which allows effective user profiling, as well as sentiment and affective analysis. The aim is to detect criminal activity and alert users and OSN operators to child predators and cyberbullies, and to reveal users under distress.
- Graph algorithms and machine learning approaches that exploit various types of OSN signals, such as friend request acceptance, likes and personal messages, to unveil

fake information with emphasis on the role of online child abusers and their patterns that can be used for detection [28], [29], [30]. This approach advances the state of the art in fake account detection, in audience boosting (e.g. fake likes or views) detection and false information propagation.

- Web-based user interfaces that discourage or prevent users from befriending suspicious OSN users, warn them or their custodians of when they are being or are about to be subjected to online abuse, and encourage them to flag malicious social web activity.
- Highly usable web-based user interfaces that discourage or prevent users from sharing sensitive content with inappropriate audiences and without the proper level of protection.
- Effective browser-based content protection (e.g. for photos or user profiles) mechanisms by employing watermarking, steganography or advanced encryption techniques [31].

In terms of end-products that can be used in proactive protection against online security and privacy risks the ENCASE architecture promotes the development of:

1) a production-grade open source OSN data analytics software stack that comprises libraries for aggressive or distressed online behavior detection, as well as fake user account, false information diffusion and audience boosting detection. The software stack will be built on the SPARK cluster computing framework [32] using large scale machine learning and graph analytics libraries. Parts of this stack will be deployed on Telefonicas (TID) Awazza web proxy[6].
2) a browser add-on that informs OSN users of whether they have befriended or are communicating with a person that is presently attempting to bully or exploit them, or has in the past exhibited aggressive behavior, or has caused other persons to exhibit emotional distress.
3) a browser add-on that enables users to be aware of whether they are communicating with a person that misrepresents its identity, and therefore its intentions, or are being the receivers of false information, or are themselves the subject of malicious false information that spreads through the network (e.g. rumors or doctored images).
4) a browser add-on that scans an OSN users content that is about to be shared in order to determine if it is sensitive, subsequently provides informative alerts, and enables the user to protect it from unwarranted leakage to unwanted recipients with easily learnable and usable interfaces.

V. Conclusion

The huge spread of the World Wide Web and the opportunities that it offers, besides the enormous advantages, poses many risks especially for children. Research shows vast adoption of the internet by children. However, the rates where children are exposed to risks vary by country, age and gender. Pornography and cyberbullying constitute perhaps the greatest risks which children are exposed to, as is an extension of the problem of real life. Online social networks and other Web 2.0 applications are at the greatest risk because they constitute the 'vehicle' through which children may be exposed to many dangers and threats.

ENCASE is a high-level software architecture designed to account for contemporary online security and privacy threats. It deviates from the static philosophy of guidelines and website-based filtering and promotes proactive and dynamic protection against these threats through intelligent content analysis, whether this is chat text, web text or information in visual form. Advanced techniques for OSN fake account identification, sexual content detection and encryption, and flagging of multiple OSN accounts of the same person will be implemented as open source tools with the form of browser add-ons.

[6]http://awazza.com/web/terms?l=en

Acknowledgment

This work is partially funded by the EC project "*ENCASE: EnhaNcing seCurity And privacy in the Social wEb: a user centered approach for the protection of minors*" under the contract H2020-MSCA-RISE-2015-691025.

References

[1] *Measuring the Information Society Report, 2015*, online at: http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2015.aspx, ITU, 2015.

[2] *Guidelines for children on child online protection*, online at: http://www.itu.int/en/cop/Pages/guidelines.aspx, ITU, 2016.

[3] D. J. Weitzner, "Free speech and child protection on the web," *IEEE Internet Computing*, vol. 11, no. 3, pp. 86–89, May/June 2007.

[4] D. Holloway, L. Green, and S. Livingstone. (2007) Zero to eight. young children and their internet use. LSE, London: EU Kids Online. [Online]. Available: http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf

[5] T. Byron, "Safer children in a digital world: The report of the byron review," Department for Education, Gov.UK, Tech. Rep. DCSF-00334-2008, April 2008. [Online]. Available: http://webarchive.nationalarchives.gov.uk/20120106161038/http://education.gov.uk/publications/eorderingdownload/dcsf-00334-2008.pdf

[6] ——, "Do we have safer children in a digital world? a review of progress since the 2008 byron review," Department for Education, Gov.UK, Tech. Rep. DCSF-00290-2010, March 2010. [Online]. Available: http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/DCSF-00290-2010.pdf

[7] *Guidelines for Policy Makers of Child Online Protection, 2009*, online at: http://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf, ITU, 2009.

[8] *Ofcom report on internet safety measures: Strategies of parental protection for children online*, online at: http://stakeholders.ofcom.org.uk/binaries/internet/internet-safety-measures.pdf, Ofcom, Jan 2014.

[9] *Ofcom report on internet safety measures: Strategies of parental protection for children online*, online at: http://stakeholders.ofcom.org.uk/binaries/internet/fourth_internet_safety_report.pdf, Ofcom, Dec 2015.

[10] M. Robinson. (2015, March) Koreas internet addiction crisis is getting worse, as teens spend up to 88 hours a week gaming. Business Insider. [Online]. Available: http://www.businessinsider.com/south-korea-online-gaming-addiction-rehab-centers-2015-3

[11] A. Lenhart. (2015, April) Teens, social media & technology overview 2015. Pew Recearch Center: Internet, Science & Tech. [Online]. Available: http://www.businessinsider.com/south-korea-online-gaming-addiction-rehab-centers-2015-3

[12] S. Livingstone, L. Haddon, J. Vincent, G. Mascheroni, and K. Olafsson. (2014) Net children go mobile: The uk report. London: London School of Economics and Political Science. [Online]. Available: https://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU\%20Kids\%20III/Reports/NCGMUKReportfinal.pdf

[13] S. Livingstone, K. Cagiltay, and K. Olafsson, "Eu kids online ii dataset: A cross-national study of children's use of the internet and its associated opportunities and risks," *British Journal of Educational Technology*, vol. 46, no. 5, pp. 988–992, August 2015.

[14] T. Woda. (2015) Digital parenting: Understanding the risk of snapchat. uknowkids.com. [Online]. Available: http://resources.uknowkids.com/blog/digital-parenting-understanding-the-risk-of-snapchat

[15] ACMA. (2009, July) Click and connect: Young australians use of online social media. Australian Communications and Media Authority. [Online]. Available: http://www.acma.gov.au/webwr/aba/about/recruitment/click_and_connect-01_qualitative_report.pdf

[16] ——. (2009, April) Developments in internet filtering technologies and other measures for promoting online safety. Australian Communications and Media Authority. [Online]. Available: http://www.acma.gov.au/webwr/_assets/main/lib310554/developments_in_internet_filters_2ndreport.pdf

[17] P. Hindley, J. Hurn, and S. Stringer, "Ward: Child protection concerns," in *Psychiatry: Breaking the ICE - Introductions, Common Tasks and Emergencies for Trainee*. John Wiley & Sons, 2016.

[18] R. Thompson, "Social support and child protection: Lessons learned and learning," *Child Abuse & Neglect*, vol. 41, pp. 19–29, 2015.

[19] *The Protection of Children Online: Report on risks faced by children online and policies to protect them*, online at: https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf, OECD, Feb 2012.

[20] S. Livingstone, "A rationale for positive online content for children," *Communication Research Trends*, vol. 28, no. 3, pp. 12–16, 2008.

[21] J. Dooley, D. Cross, L. Hearn, and R. Treyvaud. (2009) Review of existing australian and international cyber-safety research. Child Health Promotion Research Centre, Edith Cowan University, Perth. [Online]. Available: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan046312.pdf

[22] A. Marwick, D. Murgia-Diaz, and J. Palfrey, "Youth, privacy and reputations," Berkman Center Research, Tech. Rep. 2010-5, 2010. [Online]. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163

[23] R. Slonje, P. Smith, and A. Frisn, "The nature of cyberbullying, and strategies for prevention," *Computers in Human Behaviort*, vol. 29, no. 1, pp. 26–32, 2013.

[24] *Child Online Protection - Statistical Framework and Indicators*, online at: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-COP.01-11-2010-PDF-E.pdf, ITU, 2010.

[25] M. Ybarra and K. J. Mitchel, "How risky are social networking sites? a comparison of places online where youth sexual solicitation and harassment occurs," *Pediatrics*, vol. 121, no. 2, pp. e350–e357, Feb 2008.

[26] *Implementing the Childrens Online Privacy Protection Act: A Report to Congress*, online at: http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf, FTC, Feb 2007.

[27] E. Bartoli, "Children's data protection vs. marketing companies," *International Review of Law, Computers & Technology*, vol. 23, no. 1–2, pp. 35–45, July 2009.

[28] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in *Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation*, ser. NSDI'12. USENIX Association, 2012, pp. 15–15.

[29] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "Compa: Detecting compromised social network accounts," in *Proceedings of the 2013 Network and Distributed Systems Security Symposium*, 2013.

[30] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in *Proceedings of the 26th Annual Computer Security Applications Conference*, ser. ACSAC '10. ACM, 2010, pp. 1–9.

[31] K. Ntalianis and N. Tsapatsoulis, "Remote authentication via biometrics: A robust video-object steganographic mechanism over wireless networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 156–174, Jan. - March 2016.

[32] I. Ganelin, E. Orhian, K. Sasaki, and B. York, *Spark: Big Data Cluster Computing in Production*, 1st ed. Wiley, 2016.