

Perspective of understanding for Children's Privacy and Security

Lina M. Cook

Department of Computer Science and Information Systems
University of North Georgia
LMCOOK4102@ung.edu

Jianjun Yang

Department of Computer Science and Information Systems
University of North Georgia
jianjun.yang@ung.edu

Ju Shen

Department of Computer Science
University of Dayton
jshen1@udayton.edu

Abstract

The thirteen years of age requirement to open any social network account does not guarantee that children under this age would not have access to social networks such as Facebook, Snapchat, Instagram, or YouTube just to mention some. The reason for this is that children want to be a part of this technological revolution, and create these accounts by lying about their age, or are aid by their parents without realizing the consequences this action might bring. While these social networks disclose that they delete information belonging to children under 13 from their databases as soon as they are aware of it, it is questionable if they are doing enough to protect children's privacy, and if they should be liable for any incident related to this issue since such is widely known, but apparently neglected. Unfortunately, by social network administrators not reinforcing the age requirement policy, and launching features that makes its user's personal information available to third parties, are indirectly exposing children with fraudulent accounts at risk of being victims of more serious ethical and social issues such as cyber bullying, and sex crimes. While it is determined that social network has little control over this issue, all which is left to do, is to provide parents with education and control of their children's social network activity interaction to protect their privacy and keep them safe.

Keywords: social network, children's privacy, ethical and social issues

1. Introduction

The majority of social network sites prohibit the enrolment of children less than thirteen years of age. This particular rule is stipulated in their terms of service policies with purpose of complying with the law. However, many children under this age requirement continue activating accounts in social networks despite the efforts that these sites make every day to keep them out. Unfortunately parents have a great contribution to this phenomenon that apparently is getting out of control. The main issue about this children interacting in these websites illegally is that their information is being distributed by these social networks to third parties making these children vulnerable of other social issues such as cyber bullying and sexual crimes.

2. The law

Participating in Social networks has become important for one social interaction, and the common banning of children under 13 in these websites is due to COPPA, the Children’s Online Privacy Protection Act, which was enacted in 1998 and finalized by a U.S. Federal Trade Commission (FTC) rulemaking in 2000, which prohibits commercial social networks to collect information from children under 13 without the written consent from their parents [1]. While social networks sites disclaim in their Terms of Service policy that no children under thirteen years of age is allow to participate in the activities these social network offer, whit the purpose of avoiding violation of COPPA, it seems that this rule is widely overlooked by users, and social network administrators as well, when every day children keep becoming members of this sites when using fraudulent information at the time of registration. In the effort r to keep this situation under control, social networks also stipulate rules that claim that any user that violating any of their rules would have their accounts deleted. However, their efforts seem to be in vain. According to a Pew Report, 46% of online 12 year old children engage in social network activities, and this number increases to 82% when 13 years old are taken into consideration [2].

3. The issue

One of the main reasons for this situation to be out of control is due to the inability of social network sites to verify children age at the time of registration. While this measure could eradicate this problem, or at least put it under control, the implementation of a system to perform such a task could cause social network sites to incur in extra expenses, legal actions, other social concerns and more serious cases of privacy issues. [1]. In the meantime, Children lye in order to gain access to these sites and in many cases, they are aid by their parents as well. The reason for parents aiding their children to open account with fraudulent information is that they think they are just helping their children to be connected with peers, have access to educational material and to be close to family members, but they are not concern much about privacy and security issues. By lying to the social networks, parent and children are blocking the protection that COPPA can offer them and this is keeping social networks for being liable for collecting information from children under 13 years of age without written consent from their parents first. Taking Facebook as an example, since it is the most popular social networks nowadays; where about 40% of their users are technically under the age of 13; that represents in United States about 7.5 million children on the red every day, and In UK 34 % 9-12 year old that have Facebook accounts. Facebook in the effort to eradicate this issue erases about 20,000 fraudulent accounts every day [3].

4. Privacy issues

In a study conducted in 2012 where over 1000 parents were interviewed about their children social network participation, as illustrated in Table 1. the findings showed that the numbers of children under 13 years of age in these social communities are considerably high.

	Child’s current age				
	10	11	12	13	14
Has Facebook account	19%	32%	55%	69%	78%

Table 1: Percentage of children of different ages with a Facebook account

As many of us are aware, once someone decides to participate in any social network, the information shared becomes public, and by accessing games and websites through these sites, this information becomes available and distributed to third parties. The information that is shared includes user IDs, contact information and friends list which later on is used by this third parties to continue promoting their products based on the profiles captured. Once this information is available to these sites, they continue advertising products that match the profile of those users [4]. The questions is: what kind of information a child under 13 years of age would have access to, if when creating his account he or she said he or she was 30 years old? In the case of Facebook, all the information that is shared in this website is used by its administrators to enrolled user in new features without previous consent. One of these features is the tagging option, where people can be tagged in pictures, but if members don't want to be tag in a particular photo, they have to take it out manually [4]. By this being said, one can infer that the age regulations and the way is currently managed compromise the privacy of millions of children under age, which in the case of Facebook or of other social networks for this matter, is not under control, and therefore they should be more conservative when making decision on sharing every bodies information to third parties. While is clear that the COPPA ACT is being violated, when these site collects and manipulates the information of these 13 years old, there is nothing the FTC can do to make the provisions of COPPA effective because the false information these children provided at the moment of registration prevent these sites from being liable for any damages these behaviors can cause. Are these sites neglecting COPPA? Unfortunately the answer is no, apparently these sites have little or no control over what information is inputted at the moment of registration. By providing false information, these children are surrendering all protections from the law. According to the president of Facebook, there has been a formal request to the FTC to modify the act and to allow children under 13 to participate freely in this websites, so this experience can become a learning one, but a final resolution has not been made on this request [4]. Unfortunately while this decision is made, more children continue accessing these sites in an unsafe an illegal manner and they continue being at risk of more severe social ethical issues such as cyber bullying and sex crimes.

	Child's current age				
	10	11	12	13	14
Mean age child joined Facebook	8.9	10.0	11.1	12.1	11.7
Parent was aware when child signed up	95%	88%	82%	82%	88%
Parent helped create the account	78%	68%	76%	60%	47%

Table 2: Mean age when child joined Facebook, and parental awareness and assistance of account creation (among parents who report child with Facebook account).

5. Other ethical issues

According to Ami Sedghi, the Child line, which is a hot line that is available to minor with the purpose of providing counselling and emotional support, reported for the year 2012-2013 that cyber bullying complains increased to 87% in chat rooms, social networks and mobile phones. The report also shows that the children that reported this kind of complaint ranged from 12-18 years old, which is a clear example of how under 13 years old are being victimized by social networks interaction [5]. As shown in figure 1. Children under the age of 13 are exposed to bullying online; this information is based on a study conducted in the UK on December 2010 between children 9 and 16 years old [6].

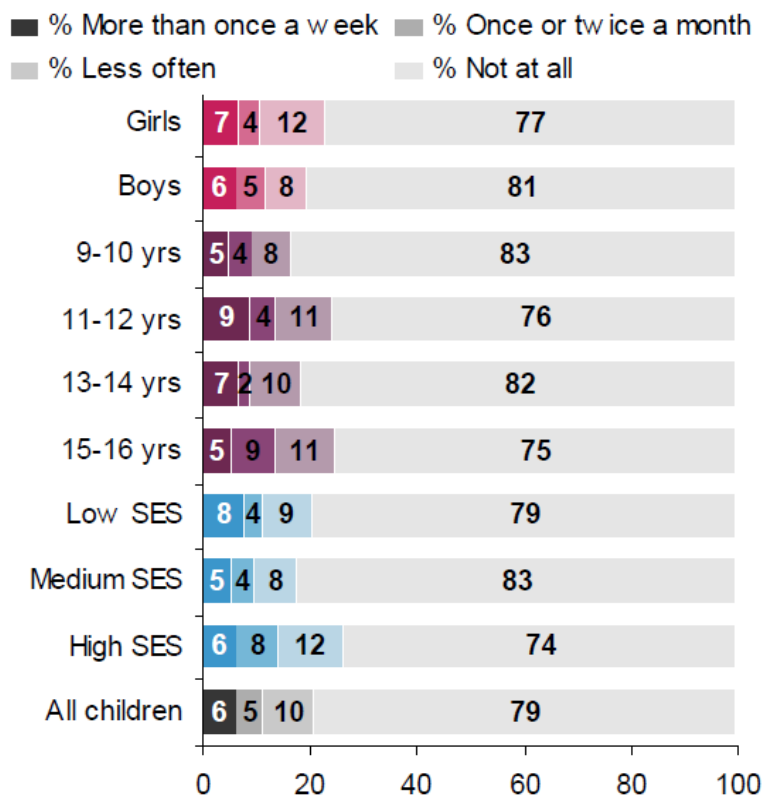


Figure 1. Child has been bullied online in a 12 month period [6].

Cyber bullying is not the only issue these children may have to confront when they are allowed to participate in these social networks. Sex crimes are also part of the problem. According to enough is enough website and its internet safety 101, in 82% of online sex crimes against minors, the offender used the victim's social networking site to gain information about the victim's likes and dislikes. 65% of online sex offenders used the victim's social networking site to gain home and school information about the victim. 26% of online sex offenders used the victim's social networking site to gain information about the victim's whereabouts at a specific time. And 13% of 2nd-3rd grade students report that they used the Internet to talk to people they do not know, 11 percent report having been asked to describe private things about their body and 10 percent have been exposed to private things about someone else's body [7]. In the same study conducted in UK in December 2010, they also reported children seeing or receiving sexual messages online, Figure 2, which again, is a clear example of how minors under the age of 13 are exposed and victimized through social networks [6].

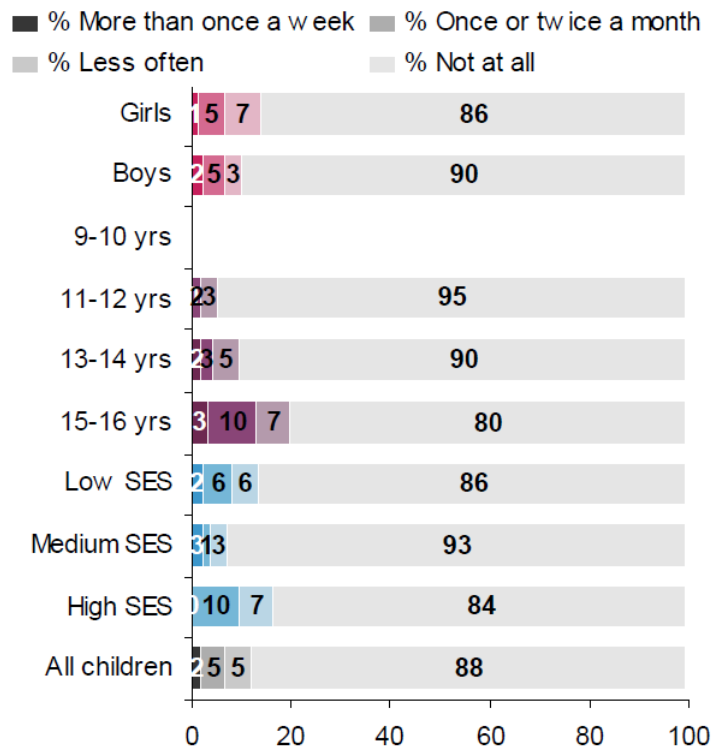


Figure2. Child has seen or received sexual messages online in a 12 months period (age 11+) [6].

6. Conclusion

It is inhabitable to continue seeing children under thirteen years of age participating in social networks. Children under the age of 13 will always find a way to get around the system opening new accounts as long as this age requirement rule stands. Although the ideal solution would be the implementation of laws to allow children to participate freely in these sites with a great load of privacy, and security features, it seems that is not a solution what will approach soon. In the meantime, social networks are not prepared to implement software to verify participant’s age at the moment of registration, but they offer tips to parent about privacy and safety online. If parent take the time to get educated about these issues and get control of their children activity online, this issue could encourage these children to engage in a more safe and responsible online activities.

7. References

- [1] Boyd, Danah, Eszter Hargittai, Jason Schultz, and John PAlfrey. "Why Parents Help Their Children Lie to Facebook about Age: Unintended Consequences of the ‘Children’s Online Privacy Protection Act’ | Boyd | First Monday." *Why Parents Help Their Children Lie to Facebook about Age: Unintended Consequences of the ‘Children’s Online Privacy Protection Act’ | Boyd | First Monday*. N.p., 7 Nov. 2011. Web. 13 Dec. 2014.
- [2] Mayers, Michael. "How Instagram Became the Social Network for Tweens." . N.p., 8 Aug. 2012. Web. 13 Dec. 2014.
- [3] Wolford, Josh. "Facebook Still Has a Big Problem with Underage Users, and They Know It." *WebProNews*. N.p., 24 Jan. 2013. Web. 13 Dec. 2014.
- [4] Reynolds, George Walter. *Ethics in Information Technology*. 5th ed. Boston: Cengage Learning, n.d. Print. p. 361-362
- [5] Sedghi, Ami. "Cyberbullying Contacts to Childline up by 87%." N.p., 9 Jan. 2014. Web. 13 Dec. 2014.

- [6] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). *Risks and safety on the internet: the UK report*. LSE, London: EU Kids Online
- [7] "InternetSafety101.org: Statistics." *Enough Is Enough InternetSafety101.org: Statistics*. N.p., n.d. Web. 11 Dec. 2014.