E-safety in Web 2.0 Learning Environments: A Research Synthesis and Implications for Researchers and Practitioners

Antigoni Parmaxi[1(✉)], Kostantinos Papadamou[1], Michael Sirivianos[1], and Makis Stamatelatos[2]

[1] Cyprus University of Technology, Limassol, Cyprus
antigoni.parmaxi@gmail.com
[2] Innovators Ltd., Athens, Greece

Abstract. This study explores the research development pertaining to safety and security in Web 2.0 learning environments, as well as a review of web-based tools and applications that attempt to address security and privacy issues in Online Social Networks. Published research manuscripts related to safety and security in collaborative learning environments have been explored, and the research topics with which researchers and practitioners deal with are discussed, as well as implications for researchers and practitioners. This paper argues that Web 2.0 learning environments entail threats and challenges in the safety of both students and instructors, and further research needs to take place for handling and protecting the privacy of all involved stakeholders.

Keywords: Security · E-safety · Social media · Web 2.0 · Social web · Social networking sites · OSNs · Literature review

1 Introduction

The advancement of Web 2.0 tools offers a rewarding source of knowledge sharing, interaction and socialization. Web 2.0 is considered "a catch-all term to describe a variety of developments on the web and a perceived shift in the way the web is used. This has been characterised as the evolution of web use from passive consumption of content to more active participation, creation and sharing – to what is sometimes called the 'read/write' web" [1, p. 9]. This term encompasses technologies that emphasize social networking, collaboration and media sharing such as Facebook, Twitter, Snapchat and MySpace. Amongst the benefits reported in the use of these tools include the development of 21st century skills such as creativity, innovation, team building, critical thinking, information sharing, higher academic achievement and improvement of ICT skills and competences [2–5]. Despite the popularity of Web 2.0 technologies, they still receive concerns by students and teachers with regard to their ability to support learning in a secure environment. Being present in online social networking sites presents particular risks such as exposure to cyberbullying, child abuse, inappropriate material and contact with dangerous strangers. Social Web can facilitate abuse of children by adults - being in place to assume fake

P. Zaphiris and A. Ioannou (Eds.): LCT 2017, Part I, LNCS 10295, pp. 249–261, 2017.
DOI: 10.1007/978-3-319-58509-3_20

identities online, a possible “danger” can intrude a child’s private zone leading to violence or even sex crimes [6]. The risks and threats that minors encounter on the internet can be classified under the following five categories [7–9]: (a) content risks: instances or events in which children are exposed to illegal harmful or age inappropriate content and harmful advice; (b) contact risks: instances or events in which children have direct interaction with other children or adults. Frequent threats under this category are cyber-grooming (i.e. adults trying to develop relationships of trust with children with the aim of having sexual intercourse with them) and cyberbullying; (c) Children targeted as consumers: instances or events in which children face the risk of being treated as consumers of products and/or services designed only for adults; (d) Economic risks: instances or events in which children spent money in gambling and other online games; (e) Online privacy risks: instances or events in which children share personal data with inappropriate audience.

A fundamental dilemma that practitioners need to address when considering the use of Web 2.0 tools for minors relates to e-safety and privacy. The question is timely in light of current upsurge of Web 2.0 technologies in educational environments, where researchers and/or instructors attempt to integrate such tools in the learning environment without violating students’ safety and personal rights. The question has attracted researchers and practitioners attention as it is evident from research papers and conferences (cf. Special issue of *Computers & Security Journal* on trust in cyber, physical and social computing). Some studies have been guided by the wish to understand students and teachers’ concerns in incorporating Web 2.0 technologies in the classroom (cf., for example, [10]) and some by the wish to identify methods for handling e-safety in a cost-effective way (cf., for example, [11]).

This paper provides the state-of-the-art regarding e-safety in the use of online collaborative environments delineating tools and threats dominant in Web 2.0 learning environments; methods and tools for handling these threats, as well as implications for researchers and practitioners.

2 Methodology

With an eye to synthesizing the findings of research regarding e-safety in Web 2.0 learning environments, we followed a three-step approach as demonstrated in Fig. 1. Our approach included: (a) compilation of the e-safety corpus which included research manuscripts related to e-safety from manual search in scientific databases; (b) refinement of the e-safety corpus and (c) synthesis of the research papers.

The methodology of this review was informed by previous studies such as Parmaxi, Zaphiris, Papadima-Sophocleous and Ioannou [4] who reviewed recent research development in Computer-Assisted Language Learning and Parmaxi and Zaphiris [5] who reviewed the use of Web 2.0 tools in Computer-Assisted Language Learning.

2.1 Development of E-safety Corpus

In order to capture scholarly activity in e-safety in Web 2.0 learning environments, we started by selecting appropriate resources which compiled the e-safety corpus.

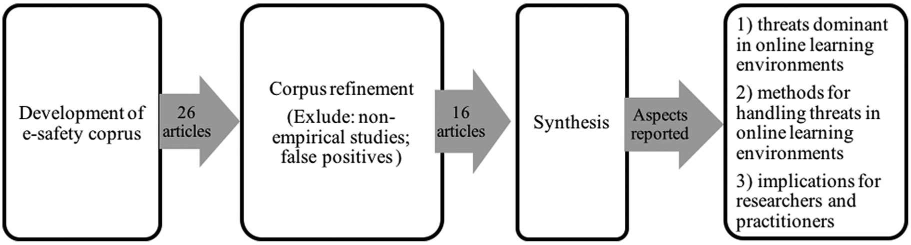
Development of
e-safety coprus
26 articles
Corpus refinement
(Exlude: non-empirical studies; false positives)
16 articles
Synthesis
Aspects reported
1) threats dominant in online learning environments
2) methods for handling threats in online learning environments
3) implications for researchers and practitioners

Fig. 1. Flow diagram of the methodology adopted for exploring scholarly activity in e-safety in online collaborative environments.

Appropriate articles for inclusion were selected via manual keyword search in manuscripts' title, abstract and given keywords. The keywords for searching were "security", "safety", "e-safety", "social media", "education", "learning", "threat", "Web 2.0" in the following databases: ERIC, Education Research Complete, Academic Search Complete, Computers & Applied Sciences Complete, Springer Link, Research Starters, Psychology and Behavioral Sciences Collection, Food Science Source, Taylor & Francis Group. The keyword search returned 26 manuscripts which comprised the preliminary e-safety corpus of this review.

2.2 Refinement of E-safety Corpus

The corpus was then refined in order to meet the objectives of this review. Each manuscript was scanned in order to elucidate the aim of each study. This stage facilitated the optimization of the e-safety corpus, as we excluded articles that were incorrectly selected in the search process (false positives) as well as articles reporting on non-empirical studies. The final e-safety corpus included 16 manuscripts.

2.3 Synthesis

Each paper in the e-safety corpus was then examined in depth, extracting information related to the following pre-defined aspects: (1) threats dominant in online learning environments; (2) methods for handling threats in online learning environments and; (3) implications for researchers and practitioners.

3 Findings

Recent debates about students' activities with Web 2.0 technologies strive between their perceived benefits and their potential threats. The social web is seen to have the capacity to foster formal and informal learning, yet students, teachers and parents demonstrate increased concern about the online risks and threats, often related to child sex abusers, and bullying, as well as concerns related to the safe presence of a school community in Online Social Networks (OSNs). Concerns about online safety fit within a broader agenda related to students' e-safety, recognizing the need to develop the skills and competences needed for taking advantage of the benefits that ICTs can provide. Figure 2 provides an overview of e-safety in Web 2.0 learning environments as derived from the e-safety corpus. The classification of the e-safety corpus demonstrated four categories that can be summarized as follows: (a) students' and teachers' attitudes and experiences towards e-safety in OSN, (b) e-safety actions, practices and policies in OSNs, (c) evaluation of schools' e-safety regulations in OSNs and (d) internet safety education.

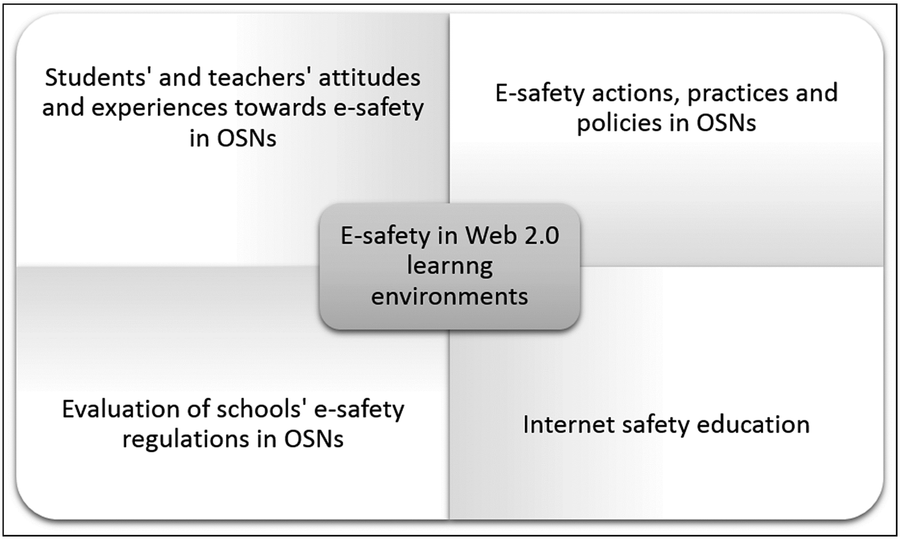
Students' and teachers' attitudes and experiences towards e-safety in OSNs
E-safety actions, practices and policies in OSNs
E-safety in Web 2.0 learnng environments
Evaluation of schools' e-safety regulations in OSNs
Internet safety education

Fig. 2. Overview of e-safety in Web 2.0 learning environments as derived from the e-safety corpus.

3.1 Students' and Teachers' Attitudes and Experiences Towards E-safety in OSNs

This category entails manuscripts that deal with students' and teachers' attitudes and experiences towards e-safety in the use of OSN. For example, Sharples, Graber, Harrison, and Logan [10] report results of a study that explored children's, teachers', parents', managers' and technical staff's understanding of Web 2.0 activities and concerns. Findings demonstrated that a high percentage of the children surveyed (74%) have used social networking sites (SNS), whilst a substantial minority interacted regularly online with people they have not met face-to-face. Although teachers demonstrated the desire to take advantage of the benefits of Web 2.0 for creative and social learning, they reported being limited by a need to show a duty of care that prevents worst-case risk to children, to restrict access to SN sites. The respondents also reported concerns about Internet bullying and exam cheating. Finally, a Policy Delphi process voiced the need for schools to allow access to Web 2.0 sites, but educate children in responsible and creative learning.

3.2 E-safety Actions, Practices and Policies in OSNs

In this category, researchers engage in online safety actions, practices and policies. For example, Searson, Hancock, Soheil, and Shepherd [12] describe the need for developing informed policies and practices that would involve a wide range of sectors of the society. Such practices would inform technology integration in educational settings addressing the following factors: national and local policies, bandwidth and technology infrastructure, educational contexts, cyber-safety and cyberwellness practices and privacy accountability. Two organizations offer examples and set guidelines for digital citizenship in educational settings, that is ISTE (https://www.iste.org/explore/ArticleDetail?articleid=101) and iKeepSafe (http://ikeepsafe.org/). On the same line, Waters [11] highlight the multifarious security challenges that school districts encounter, using as a stepping stone the example of a high school's page that has been hijacked by a former student. The manuscript concludes by suggesting two web browser add ons -Firesheep and BlackSheep- for users on unsecured WiFi networks to identify the social networking sessions of others on that Network. Similarly, the Parent Teacher Association demonstrates its action in educating children and parents about Internet Safety [13]. On the same line, Ramnath [14] discusses how school administrators can protect students' safety while integrating technological advancements in teaching and learning. The study engages in topics such as cyberbullying and cyberstalking, the use of social networking sites for collaboration and the use of Mobile Device Management for the safety of mobile devices within and outside the school network. Similarly, Campbell-Wright [15] examine e-safety in e-learning, the benefits and dangers of online interaction and guidelines for preparing organizations to handle e-safety. Similarly, Wespieser [16], upon a survey distributed in 14,309 young people in London, demonstrated the high percentage of internet usage and social network sites, as well as issues of bullying and exposure to inappropriate material. The British Educational Communications and Technology Agency (BECTA) investigated the use and impact of Web 2.0 technologies in and out of school [10]. Findings demonstrated that at Key Stages 3 and 4, students harness extensively Web 2.0 outside of school, and for social purposes. The major challenge for schools in considering the usage of Web 2.0 technologies is how to support children to engage productively and creatively in social learning while protecting them from potential risk. Most learners demonstrated awareness of internet dangers, though many performed poorly in e-safety (e.g. in practice around password security). Whilst parents are generally positive in the use of technology for learning, yet concerns about e-safety exist. The paper concludes with indicating schools' responsibility in raising children's awareness on safe engagement with Web 2.0 and the internet in general. Triggered by educators' fear to adopt social networking in their teaching, Blazer [17] sets off to review the opportunities and challenges associated with education-based social networking, providing recommendations for schools when they are establishing social networking policies. Despite the risks that schools encounter when exposing students in social networking sites, their use in the classroom can promote academic learning and increase student engagement. Recommendations provided include the formulation of strong policies that address harmful online interactions and provide educators and students with guidance in the use of OSNs. Moreover, non-commercial sites are available and can monitor access to social media. Crook and Harrison [1] also capture the importance to distinguish the current fears of society from evidence of actual risk to children. They demonstrate that the majority of learners in Key stages 3 and 4 are aware of online safety, yet, they demonstrate the need for schools and teachers to have a key role in students' e-safety. Experts participating in the study favored the empower and manage approach, i.e. schools to allow free students' access to public Web 2.0, but children need to be educated on how to use Web 2.0 activities for responsible and creative learning. Children's web activity needs to be monitored for action to be taken against threatening or unsafe online behavior. Similarly, Sutton [18] provides 7 things to know right about campus security: (a) address sexual assaults on campus; (b) develop a social-media network for resources and campus security officials; (c) increase awareness of law enforcement in the higher ed community; (d) provide Web training on current topics; (e) develop crime prevention programs that are customizable; (f) put into place adequate social-media policing policies; (g) understand what the new Violence Against Women Act (VAWA) requirements mean for your campus.

3.3 Evaluation of Schools' E-safety Regulations in OSNs

Being in place to understand and evaluate schools' e-safety regulations is an issue that attracts high interest from researchers. On this line, Lorenz, Kikkas, and Laanpere [19] analyzed the types and sources of safety incidents, the solutions offered, the students' reactions from these incidents and the solutions suggested by students. Findings demonstrated that many students do not understand what e-safety is, assuming that they are not involved in any way in an e-safety episode, even if they have suffered from an online attack. The awareness training about "stop-block-tell" does not work as it is radically different from the way students think and act in real life situations. Blocking unwanted material is the least successful solution for the students, even if current typical awareness training is focusing on it. As findings demonstrated, students seem to be passive reactors to any malicious behavior, thus training focusing on stop-block-tell" or "don't click everywhere" seems unsuccessful. The solution provided by authors "is to include more technical and other practical aspects in the awareness training and distribute step-by-step, common-language how-to-s like how to set one's privacy settings, how to report a page, picture, video or how to behave when someone is being bullied, or what to do when one becomes a victim of fraud or slander. The awareness in these areas is also needed for the adults who are setting the standard how their students or children behave and deal with the problems in the future" [19, p. 336]. Ultimately, it is of major importance for schools to develop policies, strategies and solutions that address the core issues of children.

Following a similar path, Lorenz, Kikkas, and Laanpere [20] explored 201 e-safety related stories presented by students (age 12–16), parents, teachers, school IT managers and police. Through the stories, typical behavioral patterns were mapped, beliefs, regulations and limitations regarding the use of social networks in schools in Estonia. The results demonstrated that few schools hold an explicit policy for e-safety issues. Yet, even these few school-level policy documents fall behind in tackling the topics which were most frequently mentioned in students' stories. Safety incidents related to cyberbullying or exposure to illegal material remain unsolved or even undetected. Schools delegate any safety incidents to parents who in turn look to schools for assistance. As a principle, e-safety policies should focus on topics with which all stakeholder groups agree being important: gaming, fraud, password, harassment, pornography and meeting strangers. Emphasis should be placed in assessing e-safety risks and how they can influence online learning activities. Similarly, Cranmer [21] reports on excluded young people's experiences of e-safety, demonstrating that the strategies they employ to manage their online safety are primitive and insufficient, thus pointing the need for developing further their online strategies and ultimately their digital literacy.

3.4 Internet Safety Education

Internet safety education is a topic that attracts researchers' interest, as advancement of technological systems calls for schools to teach children to protect themselves on the web. Whilst internet safety was introduced with some "special occasion" events or a dedicated "Internet Safety Day", yet these actions seem to serve no purpose and have no real learning impact [22]. On this line, Naidoo, Kritzinger, and Loock [23] present a cyber –safety awareness framework that introduces cyber safety awareness education to primary school children in the South African community. The cyber safety awareness framework offers multifarious benefits for bridging the lack of cyber safety awareness both in schools and in communities. The framework proposes that schools are grouped into clusters, with a cluster coordinator as its head. Cyber safety awareness information is expected to be disseminated through workshops attended by teacher representatives of these school clusters, and distributed back to parents, children, other teachers and ultimately to their communities. On the same line, Orech [22] elaborates on the Digital Citizenship Project that aimed at integrating Internet Safety in the educational curriculum. Through the programme, students learned about cyberbullying and prevention as well as strategies for protecting themselves in case of a cyber-insult. The project had successfully employed social media for engaging middle school teachers and students to discuss about netiquette, digital citizenship, cyber crime prevention and managing digital footprint. Ultimately, sophomore students and teachers become cybermentors engaging in conversations about cyberbullying prevention and protection. Following a somewhat similar path, Moreno, Egan, Bare, Young, and Cox [24] consider internet safety education of vital importance for youth in US, thus they surveyed at what age should such education begin and what group is held responsible for teaching it. Having distributed their survey to 356 teachers, clinicians, parents and adolescents they demonstrated that the optimal age for internet safety education is 7.2 years (SD = 2.5), whilst parents were identified as the stakeholder with the primary responsibility in teaching this topic. Clinician's role was also recognised as vital in providing resources, guidance and support.

3.5 Implications for Researchers and Practitioners

As the usage of Web 2.0 technologies advances, the more instructors and students engage with these technologies in and out of school. Internet usage has changed the way literacy is perceived and taught, raising the crucial need not only for information literacy, but also for digital literacy and specifically e-safety education. In this endeavour, the question of how parents and educators can accommodate children's behaviour on the net still needs to be further investigated. Prohibiting the use of OSNs, blocking the use of unwanted material or even blocking the use of internet in the school environment is the least successful solution. As noted by Lorenz, Kikkas, and Laanpere, [19] there is a need for more technical training; as well as more automated solution that would set one's privacy settings, instructing on how to report a page, picture, video or how to react when someone is being bullied. Taking into consideration the high percentage of internet usage and social network sites, there is a strong need in engaging children productively, responsibly and creatively in social learning while protecting them from potential risks. Whilst children are aware of internet dangers but perform poorly in applying e-safety, rises schools' responsibility in raising children's awareness by providing cyber-safety and cyberwellness practices. Thus, providing online and on-site training for both teachers and parents for confronting the challenges of the new digital era with practical guidelines on e-safety and privacy is vital. With this in mind the next section provides a review of existing web-based tools and mobile applications that attempt to address security and privacy issues in Online Social Networks.

3.6 Security and Privacy Enhancing Web-Based Tools Review

This section provides a review of existing web-based tools and mobile applications that attempt to address the security and privacy issues in Online Social Networks. The tools below are of particular interest to parents and teachers.

Qustodio (https://www.qustodio.com/en/) is a parental/educator control software available in most of the platforms [25]. It enables parents/educators to monitor and manage their kids' web and offline activity on their devices. It also allows parents/educators to track with whom their children is communicating in OSNs and manage their whole OSN activity. In addition, Qustodio can be used as a sensitive content detection and protection tool.

Avira SocialShield (http://www.avira.com/) is a Social Network Protection application developed by Avira [26]. It is a monitoring tool that inform parents/educators of their children's online activities. It monitors and checks their child's social network accounts for any comments, photos etc. that may influence the child's reputation in a negative way or may indicate that the child is in danger. Furthermore, SocialShield is able to protect the children from cyberbullying, to prevent them from participating in online discussions with inappropriate content and it is also able to verify the identities of the child's online friends.

Web of Trust (WoT; https://www.mywot.com/) is a safe browser extension for website reputation rating that helps users to make informed decisions about whether to trust a website or not when browsing online [27]. In order to provide its users an extra layer of security against malicious links posted by malicious users, Facebook uses WoT's reputation data to inform users about low reputation links.

WebWatcher (https://www.webwatcher.com/) is a parental/educator control, cross-platform compatible, monitoring software [28]. It is able to capture the content of emails and instant messages in OSNs, as well as actual keystrokes and screenshots. It assists parents/educators in keeping their children safe online by viewing what is captured in their child's screen from everywhere.

Cloudalc WebFilter Pro (http://www.cloudacl.com/) is a cloud-based content filtering application [29]. Cloudacl monitors billion of web pages to protect families and especially kids from malicious attacks and threats and to ensure a safer Internet surfing. It blocks web pages, spam servers and adult material.

Abuse User Analytics (AuA) is an analytical framework aiming to provide information about the behavior of OSN users [30]. This framework processes data from users' activities in the online social network with the goal to identify deviant or abusive activities through visualization.

FoxFilter - THE Parental control for Firefox (https://addons.mozilla.org/en-US/firefox/addon/foxfilter/) is a free browser add-on produced by Mozilla and is known as the parental control for Firefox browser [31]. It is a personal content filter that helps blocking pornographic and other inappropriate content. A user can block content for an entire site or enter custom keywords filters that will be used to block content for any site that contains these keywords.

Parental Control and Web Filter from MetaCert is a parental control browser add-on that blocks pornography, malware and spyware [32]. It protects kids and adults across multiple categories. It allows users to choose among two main categories (extra strong for kids and strong for adults) while also allows to define the specific categories that you prefer to be protected (such as Bullying, Drugs, Aggressive behavior, Gambling, Sex etc.).

MetaCert Security API (https://metacert.com/) is a Security REST API [33]. It provides a layer of security on top of web applications so the application can protect users from Phishing, Malware and Pornography.

eSafely (http://www.esafely.com/) is a parental/educator control browser add-on that provides kid-safe access to popular web resources, free of adult content [34]. Generally, it offers the following: (a) Kid Safe Facebook that protects children against threat of cyber-bullying by replacing harassing messages with friendly icons in Facebook chat; (b) Kid Safe Images that when a site is identified as hosting adult content it replaces the images with images more suitable for children; (c) Kid Safe YouTube; and (d) Kid Safe Search.

ReThink (http://www.rethinkwords.com/) is an non-intrusive, patented software product that stops Cyberbullying before the damage is done [35]. When a user tries to post an offensive message on social media, ReTHink uses patented context sensitive filtering to determine whether or not it is offensive and gives the adolescent a second chance to reconsider their decision.

PureSight Multi (http://puresight.com/) is a monitoring and filtering cross-platform software that allows children to use the internet without fearing bullies or harassment and keeps parents/educators in the know [36]. It features Facebook/Cyberbullying protection, Web filtering, Reports and alerts, file sharing control and parent/educator portal.

MM Guardian Parental Control app (http://www.mmguardian.com/) is a mobile application that allows you to block incoming calls and texts, monitor alarming texts and control which apps on the device can be used and when on a children's' smartphone [37]. It also allows the parent/educator to locate and lock his childrens' mobiles with a text message, as well as to set time restrictions to limit their use.

Funamo Parental Control app (https://www.funamo.com/) is a mobile applications that allows parents/educators to monitor their childs' mobile devices [38]. Contacts, calls, SMS, browser history, applications and locations will automatically be logged and history data is uploaded to Funamo server each day. It also allows parents/educators to enable safe search engines in the web.

Kids Place is a mobile application that allows parents/educators to choose what their children can do with their mobile device [39]. It requires from the parent/educator to set up a pin when he first login to Kids Place that is then needed to exit the app. This make sure that the kids are restricted to only use apps chosen by the parent/educator. In addition, allows the parent/educator to block incoming calls and disable all wireless signals when the app is running.

AppLock is a parental/educator control mobile application for android platforms [40]. It allows parents/educators to lock SMS, contacts, Gmail, Facebook and any other application to protect their privacy. It also allows them to lock specific photos or videos meaning that they can only access them with a code.

Screen Time Parental Control app is a parental control mobile application that empowers parents to monitor and manage the time spent on their children devices and to set time limits on selected apps, as well as a bedtime curfew, lights out and school time curfews [41]. The app runs in the background of the mobile device and it can be controlled via any web browser.

4 Conclusion

As the Internet and Communication Technologies expand rapidly in many everyday activities, concerns are raised with regard to the safety of a vulnerable group such as children on the web. As noted by O'Brien, Budish, Faris, Gasser, and Lin [42], cybersecurity incidents are reported each year sitting at the top of government policy and boardroom agendas. Our findings demonstrate that recent research activity related to safety in Web 2.0 technologies pertains to: (a) students' and teachers' attitudes and experiences towards e'-safety in OSNs, (b) e-safety actions, practices and policies in OSNs, (c) evaluation of schools' e-safety regulations in OSNs and (d) internet safety education.

The incorporation of OSNs in the classrooms confronts educators with new opportunities and challenges as there is an increasing need for educating children on productive, creative, safe and responsible engagement in the use of OSNs. More work is needed in the provision of online and on-site training of both teachers and parents for confronting the challenges of the new digital era and for putting together a comprehensive e-safety framework in order to include practical guidelines on e-safety and privacy. Blocking the use of OSNs in the school environment provides only a shallow solution to the problem; there is a need for providing students the skills for managing potential risks on the web by properly setting their privacy settings, reporting inappropriate material and reacting to cyber threats.

Moreover, there is an urgent need for designing effective measures against internet risks and threats, as well as for understanding minors' activities online. Most of the existing parental/educational control software rely on monitoring and parent/educator review to detect any abnormal activity. Some of them search for keywords to create alerts, while some others block the usual list of websites. Cyber-bullying, cyber-grooming, and exchange of sensitive content is not intelligently detected by existing web-based tools and this has a negative social effect on the children i.e. they are monitored to an excessive degree and this will probably lead them to find alternative ways to go online. Existing Internet filtering techniques for protecting minors online need to be redesigned and reapplied in a smarter way, by incorporating more sophisticated techniques such as data analytics, advanced content analysis and data mining techniques that could allow for OSN fake account identification and sexual content detection.

5 Limitations

The limitation of the e-safety corpus to the specific databases meant that some manuscripts that relate to e-safety were not included. The aim of this study in not to provide an exhaustive review of the literature pertaining to e-safety in OSNs. The results and implications derive from this particular corpus; however, findings may also reflect both present and future trends.

Acknowledgments. This research has been fully funded by the European Commission as part of the ENCASE project (H2020-MSCA-RISE of the European Union under GA number 691025).

References

1. Crook, C., Harrison, C.: Web 2.0 technologies for learning at key stages 3 and 4: summary report (2008). http://dera.ioe.ac.uk/1480/1/becta_2008_web2_summary.pdf
2. Wright E.R., Lawson A.H.: Computer-mediated communication and student learning in large introductory sociology courses. In: Paper presented at the Annual Meeting of the American Sociological Association, Hilton San Francisco & Renaissance Parc 55 Hotel, San Francisco, CA (2004). http://citation.allacademic.com/meta/p_mla_apa_research_citation/1/0/8/9/6/pages108968/p108968-1.php
3. Green H., Hannon C.: TheirSpace: Education for a Digital Generation. Demos, London (2007). http://dera.ioe.ac.uk/23215/1/Their%20space%20-%20web.pdf
4. Parmaxi, A., Zaphiris, P., Papadima-Sophocleous, S., Ioannou, A.: Mapping the landscape of computer-assisted language learning: an inventory of research. Interact. Technol. Smart Educ. **10**(4), 252–269 (2013). doi:10.1108/ITSE-02-2013-0004
5. Parmaxi, A., Zaphiris, P.: Web 2.0 in computer-assisted language learning: a research synthesis and implications for instructional design and educational practice. Interact. Learn. Environ., 1–13 (2016). doi:10.1080/10494820.2016.1172243

6. Wolak, J., Finkelhor, D., Mitchell, K.J., Ybarra, M.L.: Online ‘predators’ and their victims: myths, realities and implications for prevention and treatment. Am. Psychol. **63**, 111–128 (2008)
7. Dooley, J., Cross, D., Hearn, L., Treyvaud, R.: Review of existing australian and international cyber-safety research. Child Health Promotion Research Centre, Edith Cowan University, Perth (2009)
8. OECD: The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them. OECD Digital Economy Papers, No. 179. OECD Publishing, Paris (2011). http://dx.doi.org/10.1787/5kgcjf71pl28-en
9. Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K., Sirivianos, M.: Cyber security risks for minors: a taxonomy and a software architecture. In: 2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP), pp. 93–99. IEEE, November 2016
10. Sharples, M., Graber, R., Harrison, C., Logan, K.: E-safety and web 2.0 for children aged 11–16. J. Comput. Assist. Learn. **25**(1), 70–84 (2009)
11. Waters, J.K.: Social networking: keeping it clean. THE J. **38**(1), 52 (2011)
12. Searson, M., Hancock, M., Soheil, N., Shepherd, G.: Digital citizenship within global contexts. Educ. Inf. Technol. **20**(4), 729–741 (2015)
13. A Safer Digital World. Our Child. **39**(5), 5 (2014). ISSN 10833080
14. Ramnath, S.: How schools can keep students safe, and on Facebook. eSchool News **18**(4), 16 (2015)
15. Campbell-Wright, K.: E-safety. NIACE (2013)
16. Wespieser, K.: Young People and E-safety: The Results of the 2015 London Grid for Learning E-safety Survey. National Foundation for Educational Research (2015)
17. Blazer, C.: Social Networking in Schools: Benefits and Risks; Review of the Research; Policy Considerations; and Current Practices. Information Capsule, vol. 1109. Research Services, Miami-Dade County Public Schools (2012)
18. Sutton, H.: Review the top 7 things to know right now about campus security. Campus Secur. Rep. **12**(4), 1–5 (2015)
19. Lorenz, B., Kikkas, K., Laanpere, M.: Comparing children’s E-safety strategies with guidelines offered by adults. Electron. J. e-Learn. **10**(3), 326–338 (2012)
20. Lorenz, B., Kikkas, K., Laanpere, M.: Social networks, e-Learning and Internet safety: analysing the stories of students. In: Proceedings of the 10th European Conference on e-Learning ECEL-2011: 10th European Conference on e-Learning ECEL-2011, Brighton, UK, pp. 10–11, November 2011
21. Cranmer, S.: Listening to excluded young people’s experiences of e-safety and risk. Learn. Media Technol. **38**(1), 72–85 (2013)
22. Orech, J.: How it’s done: incorporating digital citizenship into your everyday curriculum. Tech. Learn. **33**(1), 16–18 (2012)
23. Naidoo, T., Kritzinger, E., Loock, M.: Cyber safety education: towards a cyber-safety awareness framework for primary schools. In: International Conference on e-Learning, p. 272. Academic Conferences International Limited (2013)
24. Moreno, M.A., Egan, K.G., Bare, K., Young, H.N., Cox, E.D.: Internet safety education for youth: stakeholder perspectives. BMC Public Health **13**(1), 543 (2013)
25. Qustodio: Protect, understand and manage your kids internet activity with Qustodio (2016). https://www.qustodio.com/en/
26. The Windows Club: SocialShield: Avira Social Network Protection for your child (2016). http://www.thewindowsclub.com/socialshield-review
27. WOT: Know which sites to trust (2016). https://www.mywot.com/

28. Awareness Technologies Computer & Mobile monitoring software (2016). http://www.webwatcher.com/?refID=lnkshr&siteID=Cty0dj6o3sgGHtU.M9eT5Zlm7qQ5Ms1ig
29. Cloudacl: Web Security Service (2013). http://www.cloudacl.com/webfilter/
30. Squicciarini, A.C., Dupont, J., Chen, R.: Online abusive users analytics through visualization. In: Proceedings of the 23rd International Conference on World Wide Web, pp. 155–158. ACM, April 2014
31. Mozilla add-on: The Parental control for Firefox (2014). https://addons.mozilla.org/en-US/firefox/addon/foxfilter/
32. Chrome web store: Parental Controls & and Web Filter (2016). https://chrome.google.com/webstore/detail/parentalcontrols-web-fil/dpfbddcgbimoafpgmbbjiliegkfcjkmn
33. MetaCert: MetaCert Security API (2009–2016). https://metacert.com/
34. Esafely: eSafely protects you where your Web filter doesn't (2014). http://www.esafely.com/
35. ReThink: ReThink (2016). http://www.rethinkwords.com/
36. Puresight: PureSight Online child safety (2010–2011). http://puresight.com/puresight-prevents-cyberbullying.html
37. Pervasive Group: MM Guardian Parental Control (2016). https://play.google.com/store/apps/details?id=com.mmguardian.childapp
38. Funamo: Funamo Parental Control (2015). https://play.google.com/store/apps/details?id=funamo.funamo
39. General Solutions and Services, LLC: Kids Place - Parental Control (2012). https://play.google.com/store/apps/details?id=com.kiddoware.kidsplace
40. doMobile: AppLock (2016). https://play.google.com/store/apps/details?id=com.domobile.applock
41. ScreenTime Labs: Screen Time Parental Control (2016). https://play.google.com/store/apps/details?id=com.screentime.rc&hl=en_GB
42. O'Brien, D., Budish, R., Faris, R., Gasser, U., Lin, T.: Privacy and Cybersecurity Research Briefing (2016)