Enhancing University students' privacy literacy through an educational intervention: A Greek case-study

Maria Sideri[1], Aggeliki Kitsiou[1], Eleni Tzortzaki[2], Christos Kalloniatis[1] and Stefanos Gritzalis[2]

[1]Privacy Engineering and Social Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, GR 81100, Lesvos, Greece
{msid, a.kitsiou, chkallon}@aegean.gr

[2]Information and Communication Systems Security Laboratory, Department of Information and Communications Systems Engineering, University of the Aegean, GR 83200, Samos, Greece
{etzortzaki, sgritz}@aegean.gr

Abstract. Social Network Sites (SNSs) have doubtlessly altered the way that social actors communicate and interact worldwide. Several researches have shown that users disclose personal information within SNSs, while expressing privacy concerns. Users' inability to protect their privacy within SNSs, despite their recorded privacy concerns, constitutes the core of "Privacy Paradox" and leads to privacy breaches or risks for themselves and other users. In order to reverse or at least minimize users' disclosure behavior so as to protect themselves, researches underline the need for privacy awareness increase, focusing on the crucial role of education towards this. This research aims to explore the effects of a long-term University-based educational intervention for enhancing students' digital knowledge and skills in order to protect their privacy in SNSs efficiently. The findings are encouraging regarding students' privacy awareness enhancement and protection strategies adoption.

Keywords: Social Network Sites, Facebook, privacy concerns, privacy awareness, educational intervention, semester course

1 Introduction

Social Network Sites (SNSs) provide opportunities for the creation of new relationships, maintenance of preexisting ties, self-presentation, investigation of other users' profiles, activation of meta-communication forms (Lee et al., 2013; Bryant et al., 2011; Kim and Lee, 2011; Pempek et al., 2009; Bargh and McKenna, 2004), while enabling both expression of identity at individual level and community building (Papacharissi, 2011). Users create profiles that represent, in a way they choose, their digital persona and share personal information with other users. At the same time, they raise anxieties about their privacy and the security of their information, though they themselves voluntarily provide this information and / or carelessly consent to its collection, ignoring that information is currently not under their control, but under the control of the organizations that possess it (Conger et al., 2013). Users' privacy circumventions may arise -in addition to those known as a result of governments' and companies' operation- from other users as well, in multiple forms of unwanted or uncontrolled publicity information, regardless the number of people to whom it was notified.

The interrelation between privacy in SNSs and personal information disclosure "*is characterized by a constant tension between confidentiality and transparency*" (Buschel et al., 2014, p. 642) and constitutes a multidimensional issue (Rains and Brunner, 2015; Bazarova and Choi, 2014; Spiliotopoulos and Oakley, 2013; Walton and Rice, 2013). The Privacy Paradox (Acquisti and Gross, 2006; Dienlin and Trepte, 2015) results from a conflict situation between people's fear and anxiety of being observable, supervised and vulnerable because of personal information disclosed and their actual disclosure behavior in SNSs.

Beyond legislation and providers' techniques for privacy protection, users' privacy awareness increase and relevant protective behavior adoption has been underlined of major importance. Consequently, privacy literacy is crucial in order for online privacy to be strengthened (Bartsch and Dienlin, 2016). Knowledge and skills are the two terms defining literacy. The first one helps to understand the key factors of SNSs and assess risks, while skills allow knowledge appliance. Knowledge and awareness are related to the selection of the information communicated, being thus associated to the perceived control over release, accessibility and use of information, while technical skills are important for users in order to confront SNSs structure, which provokes disclosure of personal information. In this frame, educational interventions and awareness campaigns providing knowledge and skills on privacy management are expected to have a positive effect on users' behavior, altering existing disclosure practices.

The rest of the paper is organized as follows. Section 2 addresses previous research on privacy literacy and educational interventions towards it. Section 3 presents the research question, the methodology, the research subject, as well as the educational intervention design. In Section 4 the research results are presented and discussed. Finally, Section 5 recalls the main findings of the research and discusses future research objectives.

2 Related work on Privacy Literacy and educational interventions

2.1 Privacy literacy

Researchers trying to interpret human behavior in SNSs investigate the factors that affect personal information disclosure and privacy concerns. Digital literacy has been recorded among other factors.

Digital literacy appears to have a positive effect on the protection of online privacy (Baek et al., 2014; Hargittai, 2009; Park, 2011), while its level has been recorded as prerequisite for understanding technical terms such as cookies, behavioral targeting and data-mining (Hargittai, 2009; Park, 2011). Trepte et al. (2015) argue that online privacy literacy is a combination of declarative and procedural knowledge. The first refers to users' knowledge about technical aspects of information protection related with laws and directives, while the second to users' ability to use strategies for individual privacy regulation and information protection. Researches (Park, 2011; Debatin et al., 2009) have focused on users' lack of knowledge and skills to protect their privacy, specifying this situation through cognitive inadequacy theory. The positive correlation between users' awareness and information disclosure decrease is supported by Benson et al. (2015). On the contrary low level of knowledge is related to the tendency or temptation to reveal personal information in order to obtain small benefits (Barnes, 2006; Gross and Acquisti, 2005; Smith et al., 2011). Online privacy literacy within the frame of digital literacy is thus crucial for users' knowledge and awareness increase as well as skills enhancement in order for them to be able to assess risks resulting from information disclosure, adopt technical mechanisms and strategies for combating cyber threats and consequently protect themselves efficiently.

Digital literacy is indicated as a basic life–skill that should be included "*in the education system, starting from quite an early age, as part of broader civic education or human development courses*" (Mendel et al., 2012, p. 116). Moll et al. (2014) state that "*educational measures aiming to extend digital literacy should directly aim to strengthen users' awareness about the extent of their knowledge*" (p. 218), while Chen (2013) underlines that they also help "*to cultivate a healthy and accurate risk assessment*" (p. 666). The education of online users regarding the consequences of their actions is also highlighted by Sheenan (2002) as a hopeful perspective in altering some of users' online behaviors. In this frame educational interventions are expected to alter the landscape in relation to privacy perception and its protection, since people will be able to recognize the unsafe behavior existing problem and hopefully take up relevant protective behavior.

Within this context, Taneja et al. (2014) argue on the obligation of schools and other educational institutions to develop programs focusing on enhancing "*individuals' beliefs related to information resource safety, information resource vulnerability, privacy concern, threat severity, privacy intrusion, work impediment, and intrinsic cost associated with the use of privacy controls*" (p. 172). Emphasis is equally given on the role of educators and teachers to launch educational programs so as to raise users' awareness (Cheung et al., 2015; Vanderhoven et al., 2013; O' Neil, 2001). Marino et al. (2016) note that educational programs focusing on prevention and intervention training should be delivered to "*young people in order to modify the way they perceive their social context, for example in terms of their peer groups, while also taking into account their individual characteristics*" (p. 55), while Lawler and Molluzzo (2010) and Vanderhoven et al. (2013) focus both on students' and parents' awareness enhancement through proper training at all educational levels.

The right to privacy is a fundamental human right, which is reflected on the international policy agenda. Specifically, in May 2012, the European Commission put forward the goals of scaling up awareness and empowerment including teaching of digital literacy and online safety in all EU schools (E.C., 2012a), while European Commission and U.S. Homeland Security Department have signed a joint declaration to work collectively to reduce the risks and maximize the benefits of the Internet for children (E.C., 2012b). Furthermore, UNESCO's declaration in Prague (UNESCO, 2003) has affirmed that Information Literacy should be an integral part of Education for All. These declarations and political actions have led to the formal inclusion of online safety framed in the broader media literacy education in the school curricula of many European countries.

2.2 Educational interventions towards privacy literacy enhancement

Although the issue of online safety has been implemented in education, researches investigating the impact of school education on privacy attitudes and behavior on SNSs are relatively recent and focus mostly on school students. Furthermore, as Vanderhoven et al. (2013) argue regarding online privacy issue "*if there is somehow attention given to the topic, it is not integrated in the curriculum or in a course, but it is rather incidental*" (p. 291). Additionally, most of the developed educational packages about safety and security do not tackle with the specific risks that users might encounter on SNSs since they mostly focus on Internet risks in general and are not theoretically grounded as few of them have been evaluated empirically (Vanderhoven et al., 2014; Vanderhoven et al., 2016). This leads to a lack of educational lines that should be taken into consideration when designing such programs (Del Rey et al., 2012).

Referring to the outcomes of educational packages that have been evaluated, Vanderhoven et al. (2014) and Mishna et al. (2010) argue that in cases when raising awareness and knowledge increase were observed, they were not followed however by risky behavior decrease, which is desirable and constitutes the ultimate goal of the intervention. This finding is consistent with the argument that media literacy education increases knowledge about the specific topic of a course, even so changes in attitude and behavior usually may not come up (Steinke et al., 2007). This inconsistency between expected and achieved goals reaffirms that there is little information about the characteristics that educational interventions should have in order to be effective both on users' awareness and behavior, as well as about the circumstances required for intervention's successful completion (Livingstone and Bulger, 2013).

Within this frame, Vanderhoven et al. (2016) proceeded to a research study aiming to "*propose a list of validated theoretical design principles for future development of educational materials about risks on SNSs*" (p. 459). Their research was addressed to teenagers of secondary education to measure possible changes regarding awareness, attitude and behavior, focusing on content, contact and commercial risks within SNSs. As the existing educational material about online safety didn't tackle all the aforementioned categories, researchers developed new packages (Vanderhoven et al., 2014). Their findings show a positive impact of the given courses on awareness, while revealing no impact of the courses on students' attitudes and a limited only impact on their behavior. This is consistent with the findings of Martens (2010) and Duran et al. (2008) who recorded limited or no effects of the education regarding safety on online attitudes and behavior. Changing privacy settings and modifying profile's personal information were the most commonly reported changes (Vanderhoven et al., 2016) as confirmed by students' answers to the question of whether they have changed something on their profile and what that was. These shifts reveal that the goal of behavior change was merely achieved (Vanderhoven et al., 2014; Vanderhoven et al., 2016). The researchers attribute courses of non-impact on attitude and of limited impact on behavior to the fact that courses lasted only for an hour and to peers influence as well, explaining that impact may be revealed later in time (Vanderhoven et al., 2014).

ConRed program also focused on users' awareness enhancement aiming to introduce familiarity with safety and personal information protection mechanisms on Internet and social networks, to reduce risks as cyber-bullying, harassment and addiction to the Internet and ultimately to "*refocus the misadjusted perception of information control in the social networks*" (Del Rey et al., 2012, p. 133). The program was designed according to the principles of normative social behavior theory and was addressed not only to school children but to the whole education community under scope, teachers and families included. The program results were positive referring to students' involvement reduce in cases of cyber-bullying and excessive Internet use showing a greater awareness of the students with reference, on one hand, to acknowledgement of information lack about how to control their own information and, on the other, the usefulness of learning and using strategies in order to increase their control over the information released as well as to keep uploaded information private (Del Rey et al., 2012).

Educational programs aiming to increase users' knowledge and awareness level are therefore significant in achieving a balance between users' recorded need for personal information disclosure during interaction with other users and their need for privacy protection. Since the concepts of privacy and privacy risk are influenced by several factors, caution should be given to design and implementation of educational interventions for digital literacy keeping in mind the economic, cultural, political differences between countries, people's needs and behavior as well (Tayie et al., 2012).

3 Methodology and Research Subject

3.1 Question Raised

Nowadays the majority of students are familiar with SNSs since teenage or even younger age, being thus the generation of "digital natives" (Prensky, 2001). Although most students use SNSs daily to communicate with others and have Internet experience, they are in their majority unaware of possible risks or ignore the results coming up from information disclosure and they don't show up privacy protective behavior even in the cases they realize that their personal information may be accessed and used by others. In this frame, Del Rey et al. (2012) underline that young people "*may be quicker and more efficient in the use of digital devices but they nevertheless need support and supervision in the psychosocial processes which take place when socializing is conducted via digital activity*" (p. 131).

Since online privacy literacy is of major importance in order for users' privacy awareness to be raised and consequently privacy protective behavior to be emerged (Bartsch and Dienlin, 2016), attention should be paid to educational interventions (Moll et al., 2014) in the context either of formal or informal Education. As far as formal Education in Greece is concerned, primary and secondary Education have already focused on the online safety issue, including the topic of security in the current curricula of Informatics (Greek Ministry of Education, Research and Religious Affairs, 2016a; Greek Ministry of Education, Research and Religious Affairs, 2016b). Nevertheless, the adopted educational approach focuses mainly on security issues regarding Internet usage in general, without addressing specifically the issue of privacy risks within SNSs that teenagers use extensively. Additionally, referring to the Greek educational material used in primary or secondary Education, it is indicated that even in cases where this is oriented to privacy issues on SNSs, the courses do not have long enough duration, since they are usually provided in one or two hours lessons. The above indicate that today, Greek students, getting at the age of adulthood, have acquired little information about privacy risks they may encounter on SNSs and are not supplied with the required knowledge and skills to confront them. This situation underlines the need for relevant educational interventions even after secondary school (Sideri et al., 2017).

In this regard, building up on previous literature and going beyond short-term educational interventions, a major research question is raised concerning the effects of a long-term University-based educational intervention for enhancing students' digital knowledge and skills in order to protect their privacy in SNSs. To address that, our research aims at providing insight to possible alteration of Greek students' privacy concerns and privacy management in Facebook (FB), as results deriving from an innovative educational intervention during the semester course entitled "Social Media: Identity, Communities and Application Environments", offered by the Department of Cultural Technology and Communication of the University of the Aegean.

3.2 Study design

Our study focused on the undergraduate curricula of the Department of Cultural Technology and Communication, since it provides interdisciplinary knowledge and skills regarding three disciplines: IT, Communication and Culture. Among the courses offered by the Department, the syllabus of the course "Social Media: Identity, Communities and Application Environments" (winter semester, 3rd year) included the required sections, in which our intervention could be structured and applied. The basic goal of our educational intervention centered around the positive effect on students' theoretical knowledge increase, technical skills strengthening and privacy awareness enhancement on SNSs.

The group of students attending this course with the probable exception of those that had attended a special non-formal education course on social media were expected to have knowledge of general scope with reference to SNSs risks resulting mostly by usage experience. This is also reinforced by the fact that the course on "Data Security in the Information Society" is offered in the last year of the graduate program of the Department.

The majority of the students were between 20-25 years old. Age has been shown to be an important factor in the perception and management of privacy (Steijn, 2014). Specifically, age has been recorded to be related to the willingness to experiment or the tension for careless operation in SNSs (boyd, 2014) as well as to privacy awareness level (Livingston, 2008; Raynes-Goldie, 2010; Tufekci, 2012; Brandtzæg et al., 2010; Van den Broeck et al., 2015). From the beginning of the intervention design we acknowledged that students at this age already acquire –in comparison to younger users- a shaped system of dispositions, tendencies, perceptions and consequently social actions, which is outlined by the concept of "habitus" (Bourdieu, 1977). Habitus was expected to be a possible obstacle in changes of students' concepts or actions, although this age group was simultaneously supposed to evaluate privacy more significant than younger users.

To evaluate the effects of this long-term educational intervention, a two-phase experimental study was conducted. The enrolled students of the specific course were asked to state voluntarily, in face-to-face structured interviews, their perceptions regarding privacy issues in FB, in two distinct phases; Phase I at the beginning of the course and Phase II after the completion of the lectures. Our study concentrated on FB among all SNSs since it is the most favored and used worldwide. Thus, basic prerequisite for participating in the study was having a FB account. From the fifty-four (54) students enrolled in the course, twenty-three (23) of them volunteered to participate in our experimental research procedures.

The semester course "Social Media: Identity, Communities and Application Environments" within which our experimental study was conducted, lasted 13 weeks (October 2016-January 2017) and was provided in three stages, accordingly to the syllabus distributed to students.

Stage 1(duration 2 weeks): Introduction

A theoretical introduction to social networking as a social phenomenon and to the development and history of the SNSs, as well as a short presentation of some of the most used Sites internationally were attempted within the first lectures.

Stage 2 (duration 4 weeks): Collaborative learning regarding Self-presentation and Self-disclosure in Social Media

The second part of the course included issues such as: i) the ways in which digital self is presented online through the disclosure or the intentional concealment of personal information, ii) the construction and the function of the online communities, iii) the development of the sense of belonging in an online group, iv) the negotiation of identity through an interactive symbolic exchange with others, v) the reputation and the recognition in SNSs, vi) the rewards and the benefits due to SNSs usage, vii) the possible costs as result of online behavior, issues regarding privacy protection and privacy paradox.

Stage 3 (duration 7 weeks): Collaborative learning regarding the impact of social media on social life.

In the third part of the course, issues related to the emergence of new behaviors and strategies within online communities were included, such as cyber-bulling or cyber-sex. Moreover Stage 3 focused on the usage of social media in the fields of education, culture, employment, economy, politics, and communities of fans or social movements, as well as on social media's effect in shaping public opinion. This part aimed to help students identify the provided opportunities within social networks in several fields, to focus on the importance of privacy and on negative consequences deriving from its circumvention.

Stage 2 and 3 topics were discussed in class, after the elaboration of the respective experiential learning activities. In each of the stages of our intervention, main instructions regarding both personal strategies and technical mechanisms were provided in order to enhance students' knowledge for the protection of their personal information. For each of the issues discussed in class, students had at their disposition educational material uploaded in the platform e-class, in which all students enrolled in the course had access. Educational material consisted of teacher's notes, papers in journals or conferences, chapters in books, videos or other material that was appropriate for the topic under discussion. The course was conducted by a member of faculty of the Department of Cultural Technology and Communication, holding a Ph.D. in Social Anthropology, whose research interest focus on human behavior within social media with emphasis on digital identity and privacy issues. However, depending to the topic discussed, lectures were also supported by the other members of the research team, all of whom they are faculty members of the University of the Aegean and hold a Ph.D. either in Informatics with specialization on Security and Privacy or in Sociology with specialization on Social Informatics.

To set-up our intervention efficiently, a pre-test was administrated to three students, including the structured interviews of Phase I and II as well as the teaching material of the course. This procedure intended to address the issues of data collection and instruments reliability, and to identify the range of students' embedded knowledge, deriving from the educational material taught. To assure external validity, two collaborating researchers verified that the course was offered accordingly to the syllabus, with special emphasis on the collaborative learning activities.

Phase I- Instrumentation & procedure

During the first week of the course, data were gathered in order to initially explore students' attitudes and representations regarding a series of privacy issues on FB. A structured interview schedule was developed and standardized, following a fixed format which was centered on FB usage and students' social capital outcomes within it, privacy settings management and disclosing information, privacy concerns as well as privacy risks, students' awareness and their strategies for privacy protection. Phase I- interview schedule included the following five sections of close-ended questions, on a 5-Point Likert scale. Additionally, a set of three items to address students' socio-demographic characteristics were included in the last part of the instrument.

1. Facebook Usage. This section, divided in two sub-sections, was designed to explore students' motivation to create a FB account and the management of their FB profile (sub-section 1), as well as their perceived social capital outcomes deriving from FB usage (sub-section 2). The first sub-section included items concerning the age at which students created their FB profile, the reason/s and the practices for its creation, as well as the time spent in FB daily. The second sub-section aimed to investigate students' perceptions on FB

social capital outcomes. These items were adopted from Internet Social Capital Scale (Williams, 2006).

2. FB Profile and Privacy Settings management. This section, aiming to explore students use of FB profile settings and privacy settings, included items referring to privacy settings activation when creating the profile, privacy settings change and profile visibility.

3. FB Self-disclosure. This section also comprised of two sub-sections, concerning personal information that students disclose directly on their profile and information they disclose on posts or other activities. The first sub-section included items with reference to information, such as real name, pseudonym, photo, address, while the second one refered to communicated information, posts comment, “Like” usage and “check in” function.

4. FB Privacy concerns. In this section, which was divided in two sub-sections, students were asked to rate their privacy concerns on a 5-Point Likert scale (extending from “not at all” to “much”) regarding a series of issues deriving from their engagement in FB. The first sub-section included items concerning the extent of worries to issues such as companies’ access to students’ personal information, personalized advertisements or phishing, while the second aimed to explore students’ concerns regarding disclosure of sensitive personal information to unwanted or unknown audience.

5. FB Privacy risks, awareness and protection strategies. This section aimed to explore students’ perceptions regarding privacy risks, their privacy awareness, as well as the privacy strategies they follow in FB. Students were asked to state their agreement or disagreement on the respective three sub-sections. The first sub-section included several items such as “There is no risk on FB” or “I realize that every move on FB leaves digital traces”, while sub-section 2 items such as “I don’t understand FB’s technical features in order to protect myself”, “I believe that anti-spyware programs are useless”. The third sub-section referred to students’ privacy strategies, using items such as “FB privacy settings are adequate to protect my privacy”.

Phase II- Instrumentation & Control procedure

Thirteen weeks after the collection of the initial data and the completion of the course lectures, the same interviewing procedure was followed in order to explore the impact of the semester course on the students. Phase II- interview schedule consisted of five sections of close-ended questions on 5-Point Likert Scale, including repeated measurements from Phase I- interview. Phase II- interview aimed to investigate possible changes regarding students’ privacy perceptions, self-disclosure behaviors and privacy management in FB, such as the adoption of stricter privacy strategies by the end of the course in comparison to the ones they previously adopted. The items of the sections are described in the following measurements:

1. Facebook Usage. This section of questions, including dichotomous items, was designed to verify students’ knowledge sources regarding FB usage, such as the ways they learned to utilize its functions (e.g. by themselves or getting help by a familiar person).

2. FB Self-disclosure, FB Profile and Privacy Settings management. This section divided to six sub-sections of dichotomous questions, aiming to examine the possible alteration of students’ disclosed information and their privacy settings management. Subsections 1 and 2 concerned the addition or the removal respectively of personal information in students’ FB profiles within the months of the intervention. The third sub-section included items with reference to possible changes in provided information, such as real name, pseudonym or photo, within the same period. Subsections 4 and 5 were developed in order to explore possible alteration regarding the restriction or the extension of students’ profile visibility within the period of intervention, using measurements such

as "Have you restricted the visibility of your profile from public to friends only?". Subsection 6 aimed to explore the alteration of students' privacy settings during the same period, as well as the reasons they motivated them to change the settings.

3. FB Privacy concerns. In this section, which included repeated measurements from Phase I- interview schedule, students were asked once more to rate their privacy concerns in order to explore if these were increased or diminished after the completion of the educational intervention.

4. FB Privacy behavior and protection strategies. This section, including items most of which derived from Phase- I interview schedule, was developed to control if students altered their privacy behaviors and their protection strategies after the completion of the course.

5. Educational Intervention Evaluation. The section aimed to explore the outcomes deriving from our educational intervention. Students were asked to rate the perceived theoretical and technical knowledge on a 5-Point Likert scale (extending from "not at all" to "much"), providing answers to measurements such as "I have understood terms like connection, interaction etc.", "I have learned how social media are utilized in different settings", "I have learned that there are plenty of privacy risks on social media". At the end of the interview, students could add any other statement regarding the evaluation of the intervention.

To conduct the students' interviews advantageously and to increase their reliability, the interview schedule both in Phase I and II was followed in the exact same order in the exact same way for each one, without following up on the interviewees' answers in. All the interviews were audio recorded and the interviewers took notes of each interview. The transcripts from the interviews were made from the audio recordings and by cross checking with the notes.

4 Discussion

To evaluate the outcomes of our educational intervention, Phase I and Phase II records were analyzed using quantitive and qualitive speech analysis and compared in order to explore possible shift concerning privacy awareness and behavior of the twenty-three students who participated in our experimental research procedures. Since our research was experimental, providing indicative but not conclusive findings, it was important for a further understanding of the research, to present at first a numeric description of students' trends and attitudes. Specifically, regarding the close-ended questions, the frequencies of students' answers were measured by researchers in order to draw conclusions on students' views, attitudes and behaviors. Descriptive statistics, including percentages, were afterwards calculated in order for the results to be presented. With reference to the one open-ended question, students' answers constituted the unit of measurement and analysis in order for the researchers to select and codify categories that compel the essential content of students' speech.

The results presented in this paper refer to the effects of our intervention right afterwards the lectures' completion due to several academic obligations that the students participating in the intervention had. This didn't allow us to conduct another interview after a period of time. So, long-term effects cannot be estimated.

The age range of the sample is 20–55, while most of them are between 20-25 years old, two between 26-35 years old and one student between 46-55 years old. The gender split is not adequative enough, since five of the students are men and the rest women.

4.1 Facebook Usage

Findings of Phase I indicate that 48% of the students had created their FB profile at the age of 15 or 16 years old, 26% at the age of 12 -14 years old, while 22% at the age of 17-22 years old, supporting Prensky's (2001) thesis regarding the generation of "digital natives". On the other hand, as it was expected, the participant aged between 46-55 years old, had created his/her profile in adulthood (41 years old).

The majority of the students (91%) stated that they created a FB profile in order to maintain and extend their relationships, as well as to have fun and entertainment. Social capital benefits, social support, users' need to belong to a group, self-promotion and entertainment have been recorded as incentives in users' modus operandi leading to self-disclosure in SNSs (Krasnova et al., 2010; Steinfield et al., 2012; Ellison et al., 2007; Taddicken and Jers, 2011; Trepte and Reinecke, 2013; Cheung et al., 2011; Utz and Kramer, 2009; boyd and Heer, 2006; Ragnedda, 2011). The impact of students' social environment is indicated also as a major factor (78%) that urged them to create a profile. This has been already recorded in literature (Cheung et al., 2015; Zhou, 2011; Ziegele and Quiring, 2011). However, it is extremely noteworthy that findings regarding students perceived social capital benefits within FB highlight some contradictories. More than half of the students (57%) declared that relationships in FB are not real, while an almost equal proportion (52%) were uncertain regarding the FB positive impact on the improvement of their relationships. These findings indicate that the correlation between students' motivations for participation in FB and their anticipated social capital benefits needs to be further explored, since it may be variously affected by other variables, such as privacy concerns. In this respect, we suggest that an effective educational intervention should include more theoretical knowledge regarding the benefits and the costs due to SNSs usage.

FB intensity usage measurements were very high, since most of the students spend at least three hours per day on FB, including some who are connected all day, while only 17% spends up to one hour. Although researchers (Stutzman et al., 2013; Trepte and Reinecke, 2013) have pointed out that FB intensive use is an important factor for the increase of self-disclosure, others (Park and Jang, 2014) have reported a positive association between frequency of Internet access and privacy knowledge. Up to this point, we assumed that the more time students spend online, the higher their online privacy literacy would be. Though this was not supported by other findings.

Regarding students' technical knowledge for the creation of their profile and FB functions, most of them (61%) stated that they had learned by themselves how to utilize it, while to 35% a friend's help was provided. Only 4% of the students were advised by family how to create their profile and act within FB. This finding indicates that parents should be more involved in these procedures since students engage with FB in adolescent. Findings of Phase I are supported by the findings of Phase II, whereby the same ratio of the students affirmed that they had discovered FB functions by themselves mainly or through help offered by a friend. It is also of great importance that in Phase II, after the completion of the semester course, students admitted not having the required knowledge regarding all FB functions. This underlines that FB intensity usage is not directly related to knowledge. Moreover, 83% of students declared that their previous formal education (primary and secondary) had not contributed to the enhancement of this kind of knowledge, while only two stated that they had tried in the past to extend their knowledge on social media usage attending an educational seminar. These findings, deriving from both Phase I and Phase II, support the necessity for the establishment of specific long-term educational measures that will reinforce students' digital literacy regarding SNSs usage and also affirm the need for educational programs targeting parents as proposed by Costello et al. (2016) and Feng and Xie (2014).

4.2. FB Profile and Privacy Settings management

Findings of Phase I reveal that most of the students (74%) had their profile visible to all, while the rest, in equally ratios (8,5%), provided visibility to friends, selected friends or friends and their friends. Findings of Phase II highlight an important shift concerning students' FB Profile management, since 65% of those who had it visible to public, restricted it to friends only, 18% to friends and their friends, and 13% to selected friends.

An almost identical shift is indicated regarding students' FB privacy settings management, comparing findings of Phase I and II. At Phase I, only 35% of the students had activated Privacy Settings when creating their Profile, 3% had not, while 52% stated either that they had not noticed the privacy settings or did not understand what they were supposed to do. Not reading privacy policy (Marwick et al., 2010) or not using privacy settings (Debatin et al., 2009; Livingstone et al., 2011) have been recorded in literature as risky behaviors. Nevertheless, in Phase II, 57% of those who had not activated privacy settings declared that they had changed them within the period of the semester course, justifying this change in the context of their goal to obtain more privacy protection within FB, as well as because of the attention they paid to the security notices that came up. Up to this, it is important to note that default privacy settings are an important tool that affect information disclosure and as Acquisti, Brandimarte and Loewenstein (2015) support, they are expected to affect individuals' privacy behavior regarding their profiles' visibility on SNSs. Consequently, privacy by default and privacy by design are gaining more and more attention towards the embedded and by default protection of users' privacy, by embedding the privacy protection mechanisms in the system per se, leaving less options to the users to change or adjust their privacy requirements accordingly. However, the main difference between privacy by design and privacy by default is that privacy by design describes all the necessary steps that need to be fulfilled in the software engineering world for a software product or service to fulfill specific privacy requirements along with its functional requirements. Privacy by default (more applicable to SNSs) is dealing with the end product and how the privacy options are already adjusted for providing maximum protection of users based on the data that the users provide for using a specific resource or service. If a service does not follow the default privacy settings and demands more private information (so more data disclosure) then a privacy incident occurs since the privacy requirements identified for the protection of users' privacy have been violated. As far as Facebook in particular concerns, even though its default privacy settings are modified within the years by embedding personal and social plugins in order to satisfy users' desires for disclosure (boyd and Hargittai, 2010), the use of the default privacy setting "Everyone", namely the users' ability to share their content with all Facebook users, results in the disclosure of a vast amount of information and content among million users and third parties, precisely due to this use (Liu et al., 2011). When the Federal Trade Commission in USA challenged FB to support its approach regarding this setting, FB emphasized on the fact that one third of total FB users edited their settings for a first time due to this setting (boyd and Hargittai, 2010). In this regard, the role of default privacy settings becomes even more significant for privacy management and towards this, as boyd and Hargittai (2010) also support, technological skills are equally important, affecting the correlation between the adjustment of Facebook privacy settings and the frequency of their use. Users with limited skills may not adjust their Facebook accounts accordingly to their desire for privacy, resulting in more exposure if the default settings lead towards this (boyd and Hargittai, 2010).

Therefore, findings are encouraging showing the positive effect of our educational intervention regarding the adoption of certain practices by students in order to protect their privacy, while literature (Ellison et al., 2011; Stutzman et al., 2012) has already shown that adjusting privacy settings provided by the SNSs are one of the strategies for mitigating the risks arising from disclosure. Furthermore, our findings emphatically support previous work (Vanderhoven et al., 2013; Sheehan, 2002) as far as the necessity of education targeted on the issue of profile and privacy settings management is concerned.

4.3. FB Self-disclosure

Findings of Phase I indicate that students had used their actual personal information in their FB profiles. Specifically, Table 1 presents the personal information the students chose to disclose.

Table 1. Personal Information Disclosed

Type of information	% of Students
real name	87%
real post address	91%
real place of residence	78%
real current studies or employment	78%
real place of birth	70%
real date of birth	70%
real phone number	43%
real previous studies or employment	17%
real e-mail address	9%
real photo	4%
real personal status	4%

Students seem to be reluctant to reveal pieces of information such as phone number, e-mail address, previous job or studies, personal status and photo, probably considering them more sensitive. The information sensitivity has been indicated as a factor which increases the perception of risk and reduces the desire for disclosure (Malhotra et al., 2004; Taddicken, 2014). During Phase II, students were asked if they had removed any of the disclosed information from their FB profile within the period of the intervention. Only 22% of them stated that they had removed personal status, 13% place of residence and previous studies or employment, 9% place of birth and postal address, and 4% birth date. These findings reveal a minor shift which is not unfamiliar in previous literature. Vanderhoven et al. (2016) support that "*the interventions may have a delayed impact on attitudes and behavior, making it impossible to completely observe the impact in the posttest scores measured immediately after the intervention*" (p. 476). Furthermore, it is indicated that our educational intervention should have given more attention to the sensitivity degree of personal information, since students disclosure may end up to unintended consequences including damaged reputation, rumors and gossip, cyberbullying, harassment or stalking, misuse by third parties like advertisers or by superiors like teachers or potential employers (Debatin et al., 2009).

As far as indirect information disclosure is concerned, both in Phase I and II, 35% of the students were recorded to share happy or unhappy moments, success or failure within FB, while posts regarding personal political beliefs are avoided (74%). Additionally, students (44%), in Phase I, declared that they usually tag other persons' names in their photos, while in Phase II, 70% admitted that this specific practice is more than familiar to them. Taking this finding into consideration, it is also indicated that special emphasis should have been given on indirect information disclosure practices.

Regarding other disclosure practices, most of the students (65%), in Phase II, affirmed that they do not any longer use the feature "Like" for product advertisements, while 87% of them had stated, in Phase I, that this practice was quite usual. This finding records an encouraging shift in students' behavior. It is also noteworthy that in Phase I all students stated that they "check in" on FB every time they visit a place, while in Phase II only 13% of them preserved this behavior. Respectively, while only 22% of the students preferred to communicate through inbox in Phase I, an obvious alteration is recorded in Phase II, whereby 91% of the students declared this preference.

It is equally of great importance, that in Phase I, all students stated that they do not have any kind of control over the information they post, while in Phase II, they all declared that they had. Information control is recognized as a key element in the perception and assumption of risk (Klein and Kunda, 1994; Nordgren et al., 2007; Brandimarte et al., 2012) that results from information disclosure. Hoadley et al. (2010) have shown that lower estimated personal information control is related to higher privacy concerns, while in cases whereby users ignore privacy, they feel that they have control over the information they reveal (Acquisti and Gross, 2006). Nevertheless, it should be underlined that most people perceive their control over information release, ignoring their control over access, use or misuse of information by SNSs and third parties, including governments (Bertot et al., 2010; Bertot et al., 2012). Furthermore, 70% of the students in Phase II expressed their certainty that their information shared will not result in troubles in the future.

These findings indicate the advantages of our educational intervention, supporting Taddicken and Jers thesis (2011) according to which users with a better school education are better able to evaluate privacy risks in SNSs than those with less experience and lower education.

4.4. FB Privacy Concerns

Findings of Phase I and II compared, indicate that our educational intervention had a positive impact on students' privacy concerns increase. While in Phase I only 35% of the students had expressed their concerns regarding personalized advertisements provided by FB, in Phase II this ratio was almost double (65%). Additionally, although in Phase I the majority of the students (82%) were not at all concerned regarding companies' ability to have access to their personal information, in Phase II, this percentage was reduced to 74%. In this respect, since privacy concerns may burden the self-disclosure process (Stutzman et al., 2013), it is indicated that our educational intervention, besides targeted advertisements, should also be more focused on companies' access to personal information through SNSs.

Most of the students (78%) in Phase I were extremely concerned regarding FB function as a space where control or violence can be extensively exercised. In Phase II this proportion was increased to 87%, indicating that the students acknowledged that SNSs may reduce free self-determination and limit privacy (Sideri et al., 2015), leading to boundary problems of the kind of information that should be shared within SNSs (Barnes, 2006).

After the completion of our educational intervention, students' anxiety centered on Phishing within FB was also recorded. Specifically, a notable shift has been shown regarding those students that had expressed moderate concerns regarding Phishing in Phase I (13%). This ratio was increased to 30,4% in Phase II. Additionally, in Phase I, some students seemed to have no concerns at all regarding other users' access to their thoughts (22%) and feelings (13%). This could be attributed to trust to other members of SNSs which has been shown to positively affect personal information disclosure (Krasnova et al., 2010; Posey et al., 2010). Findings, in Phase II, show a positive alteration only regarding access to students' thoughts -this percentage was reduced to 13%- while the respective ratio regarding their feelings was increased to 17%. In this respect, considering that the expression of innermost thoughts and feelings has been indicated as a reason for students' participation in SNSs (Sideri et al., 2015) in order for them to respond to the anticipated socio-emotional outcomes without understanding possible risks though, our educational intervention should have given special emphasis on this issue.

It is of great importance also that 70% of the students declared in Phase II that their concerns regarding profile visibility were reduced, since, after the completion of the course, they had restricted it into specific groups. An equal shift has been recorded for their concerns regarding unwanted audience knowledge about their location and their activities, since they avoided to "check in" and communicated through their inbox by the end of the course.

The above findings indicate an explicit impact on students' privacy awareness deriving from our intervention and support previous work (Johnson et al., 2012) regarding the usefulness of privacy control techniques that allow users to successfully manage privacy threats from unknown external audience.

4.5. FB Privacy Risks

Findings of our study indicate that our educational intervention achieved to a great extend to raise students' awareness about the potential risks of self-disclosure in SNSs, helping them to understand the key features of SNSs function and assess the possible risks deriving from their usage. In many cases, users in order to utilize SNSs services have to reveal personal information according to the presets of SNSs function (Ziegele and Quiring, 2011; Stutzman et al., 2013; Nguyen et al., 2012; Gibbs et al., 2011). As shown, perception about SNSs safety impacts on privacy concerns (Acquisti and Gross, 2006).

During Phase I, 61% of the students declared that they didn't deal with any risk within FB, while in Phase II, 74% of the sample admitted having been conscious of the multiple risks that they could face within FB. It is noteworthy that in Phase I, none of the students had realized that all their actions in FB are leaving digital "traces", are recorded and detected, while most of them (78%) supported that if they deleted a conversation, no one would be able to find it. However, in Phase II, the majority of them (87%) understood that their previous perceptions were misguided. Students' low level of awareness at the beginning of the course results, probably, from their stated lack of knowledge regarding FB functions, which is a crucial factor in order for users to capture the nature of the FB risks.

Furthermore, the majority of the students (83%), in Phase I, were not aware of the fact that FB as a provider gathers users' personal information, supporting previous work (Lawler and Molluzzo, 2010) which points out that students do not read SNSs privacy policies and therefore they do not realize that their personal information might be gathered, used and shared by the providers. Though, in Phase II, the majority of the students (87%) declared that they had acknowledged this risk. Users' confidence in service providers has been shown to positively impact on information disclosure (Cheung et al., 2015; Dwyer et al., 2007). Besides the fact that FB gathers users' personal information, 83% of the students in Phase II acknowledged that governments may also have access to their personal information through FB, while in Phase I, only 61% of them shared this perception.

These findings show, supporting Chen (2013) thesis, that the educational material referring to SNSs' function and risk assessment may provide the appropriate cognitive tools in order to remove the respective bias regarding the issue.

4.6. FB Privacy awareness and protection strategies

Findings of our study highlight that the offered semester course enhanced students' awareness in order to identify and adopt specific protection strategies related to personal information disclosure behavior. These strategies are either personal and concern students themselves or related to privacy control techniques provided by the Site.

As far as control techniques related to FB are concerned, all students stated in Phase I that they acknowledged its technical functions. However, in Phase II, 69% of them demonstrated that they had become aware of possible dangers deriving from FB technical characteristics that they didn't know before. This finding supports previous work (Nguyen et al., 2012) by which it is indicated that users would be more able to protect their privacy if the provided mechanisms and interfaces allowed them to understand their function and if these mechanisms were incorporated in users' practices and values. In this respect, while in Phase I, 35% of the students believed that FB privacy settings are adequate to protect themselves, 69% expressed their anxiety regarding the usefulness of the specific protection strategy in Phase II. Previous literature (Cheung et al., 2015) has already suggested that SNSs providers should introduce more features and privacy indices that will allow users to better comprehend their current privacy protection level and the potential risks as well. As Marwick and boyd (2014) also support, SNSs adopt specifically legal and technical instantiations, which are usually based on oversimplified analysis of individual behavior. So, even though SNSs providers meet typically their responsibility to preserve users' privacy, these legal and technical precautions are usually ineffective (Külcü, & Henkoğlu, 2014) failing to address users' complex privacy behaviors. Respectively, it is not surprising that privacy policies within SNSs are differentiated year to year. Therefore, in order for the SNSs providers to adequately undertake their responsibility to preserve users' privacy a more efficient social, legal and technical requirements should be established (Marwick & boyd, 2014; Külcü, & Henkoğlu, 2014).

Furthermore, our findings point out that while 26% of the students, in Phase I, were not sure about the usefulness of the anti-spyware software, in Phase II this ratio was reduced to 21%, highlighting once more the impact of our intervention.

As far as students' personal protection strategies are concerned, findings indicate that most of the students in Phase I supported that they themselves have the responsibility to protect their privacy within FB (70%), as well as to protect others (96%), by utilizing several personal strategies. However, in Phase II, 56% of the students admitted that they didn't have in the past the required knowledge to achieve that, supporting previous research results (Del Rey et al., 2012) that record the necessity for students to learn various strategies for augmenting their information control in SNSs. Some of these strategies refer to the choice of the information type students post in their profile, to the updates they share in their Status (Ellison et al., 2011) or to the control of their network (Stutzman et al., 2012; Kramer and Haferkamp, 2011). It is notable though, that findings, both in Phase I and II, show that the majority of the students strongly believed that their friends cannot protect their privacy within FB and are not willing to follow that kind of strategies. Taking this into consideration, our educational intervention should be more focused on interactive protection strategies between students and their friends.

It is also noteworthy that while, in Phase I, 56% of the students declared that they didn't have the skills to block unwanted audience out of their profile, in Phase II, 61% of the total sample affirmed that they had acquired these. Additionally, while in Phase I, 22% of the students declared that they had visited suspicious pages through FB, this ratio was reduced to 4% in Phase II. Respectively, findings point out the positive effect of our educational intervention regarding the adoption of the specific strategies.

Finally, students' awareness was explored regarding current legislation for privacy protection in digital environments. Even though 78% of the students stated, in Phase I, that their privacy within FB could be protected via legislation, only 13% of them declared in Phase II that they are familiar with current legislation relatively well. It must be noted that students were supplied with material to read regarding Greek legislation and EU directives concerning data protection and were instructed to access relevant websites such as the one of EU or the Hellenic Data Protection Authority. Nevertheless, no special lecture regarding legislation was elaborated or thorough information regarding General Data Protection Regulation (GDPR) was provided and this, as findings show, constitutes a problem that it should be taken into consideration in future interventions. Focusing on GDPR would provide students with a further understanding of users' new rights and protection strategies within SNSs. GDPR, by gaining rights, such as erasure of data- right to be forgotten, empowers users to have a better control of their information within SNSs, since users can request the permanent erase of their personal information from the SNSs servers, while SNSs or other third parties must erase these information, if they are no longer necessary in relation to the purposes for which they were collected or processed (Shoor, 2014; Thesis, 2014).

4.7. Educational Intervention Evaluation

Our study was completed gathering data regarding students' evaluation related to their perceived outcomes deriving from our educational intervention. Findings indicate that all students affirmed that they enhanced their knowledge in a theoretical basis by capturing and clearly defining the concepts of "social media", "digital identity", "interaction", "connection", "self-disclosure", "privacy", "privacy concerns", "privacy risks", "privacy settings", "privacy awareness" and "privacy protection strategies". The majority (96%) also declared that they acknowledged the operation and the utility of social media within different socio-economic environments and fields as those of politics, culture, journalism or market. The same majority affirmed that became aware not only of the benefits deriving from social media usage, but also of the risks related to them, both in a theoretical and practical aspect. Furthermore, most of the students (96%) recognized the continuous digital observation as a major risk that emerges from social media increasing usage. This perception has already been highlighted in previous literature (Barnes, 2006; Norris, 2003) whereby FB has been indicated as a new field of social conflicts among individuals characterized by different forms of exercised social control.

One of the most important outcomes of our educational intervention, as findings show, concerns awareness enhancement. The majority of the students (91%) acknowledged the necessity to maintain an adequate balance between their desire to interact with other people and obtain specific benefits within SNSs and their need to protect their privacy. In this respect and as basic cognitive outcome, 87% of the students declared that, after the course, they were more conscious of the practices that should adopt when acting in SNSs.

Furthermore, within the frame of Phase II each student was asked to provide any additional information by the end of his/her interview evaluating the outcomes of the intervention. Some of their quotes, following below, are extremely indicative regarding our educational intervention impact. One of the students emphatically stated: "I have learned that I must think twice what might be hidden behind a profile or a post. Furthermore, I realized that having the right to speak freely, doesn't mean that we can write whatever we want. Our freedom ends where others' rights start". Emphasis on profiles' authenticity was given by another student stating "I have doubts related to the authenticity of several profiles in social media", while others referred to privacy concerns in social media: "Our personal information must be protected" and "I realized that I cannot protect myself in social media". Two other students referred to caution and prudence: "I understood that Internet and its applications should be used with prudence" and "I realized that I should be more careful posting on FB". Finally, two other students stated: "I understood how individuals and Institutions can operate within online communication platforms, but I have also learned how to present myself without risking" and "We should not concern ourselves with social media in that extent, since there is the offline personal life too".

5 Conclusion

The current study, based on the existing literature and going beyond this, concerned an educational intervention that focused on enhancing students' privacy awareness within SNSs and it was addressed at a group of Greek University students, enrolled in the course titled "Social Media: Identity, Communities and Application Environments", offered by the Department of Cultural Technology and Communication of the University of the Aegean. The study, structured in two experimental phases, aimed at exploring potential shifts regarding students' privacy concerns and awareness that would lead respectively to potential behavior shift.

This educational intervention differs from previous ones, with reference to its duration, target group and context. In contrast to former short-term relevant interventions, the current lasted 13 weeks and it was based on the design principle that such educational programs should simultaneously emphasize, namely on "*positive aspects of SNS, while informing about the possible risks*" (Vanderhoven et al., 2013, 291). The long-term intervention was implemented considering that attitude's and behavior's shifts require time in order for the participants to evaluate new knowledge through cognitive processes, to incorporate this into their system of practices and to manifest new behaviors. Unlike to former interventions, it was addressed to University students, taking also into account that the educational material of the course of Informatics of primary and secondary Greek Education, in which previous interventions focused, does not specialize on SNSs. The age group, on which our intervention focused, acquires already –in comparison to younger users e.g. school students- a shaped system of dispositions, tendencies, perceptions and consequently social actions ("habitus"), which was expected to be a potential obstacle in changes regarding students' concepts or actions. On the other hand, estimating that this age group evaluates privacy as a significant human right and it is likely to apply stricter privacy settings on SNS (Debatin et al., 2009), the embedding of new knowledge, covering previous cognitive gaps, was expected to have an impact on their concepts and actions.

The results of our research pointed out that the majority of students had created their profile on their adolescent, while literature has shown that FB intensity usage impacts positively on knowledge. However, students were not familiar with FB functions, while their previous formal education had not contributed towards this. In this respect, the need for the establishment of specific long-term educational measures is pointed out. These measures will reinforce students' digital literacy, regardless FB intensity usage, in order for students to cover knowledge gaps resulting from previous educational training. Our study has also highlighted that students include in their profile actual personal information which they didn't remove within the period of the intervention, indicating that behavior changes may come up later in time or due to students' "habitus". This underlines the need for an ongoing monitoring of online behaviors. Regarding information that students were reluctant to reveal (e.g. phone number, photo of their own), considering it as more sensitive, future researches should focus on revealing users' concepts on information sensitivity, since it is affected by many factors both socially and individually defined. With reference to indirect information disclosure, students' practice of tagging other persons' names in their photos didn't change after the completion of the intervention and therefore emphasis should be given during educational interventions on indirect information disclosure practices. Thus, an encouraging behavior shift was recorded regarding the feature "Like" for several products advertisements and the feature "check in" FB's function, inbox communication and information control. Although, at first, all students stated not having control over the information they post, this was subverted after the course. This clearly shows that our educational intervention helped students to acknowledge relevant risks and confront them.

Privacy concerns increase was also recorded regarding personalized advertisements provided by FB, FB's function as a space of exercised control or violence and phishing, while students' concerns regarding companies' access to their personal information were decreased a little, indicating the necessity for the educational material to be more focused on this issue. Referring to students' concerns about other users' access to their thoughts and feelings, the ratio of those "not concerned at all" was reduced regarding thoughts only. This non-subversion practice can be seen in terms of social developmental goals that characterizes students' life stage (Arnett, 2000) or of habitus, indicating that future educational interventions should focus on outlining risks resulting from feelings disclosure. It is important to note that the students had acquired skills in order to block unwanted audience out of their profile, and therefore the goal of privacy awareness enhancement through our educational intervention was accomplished.

Additionally, the current educational intervention achieved to a great extent to raise students' awareness about the potential risks of self-disclosure in SNSs, by helping them to understand the key features of SNSs' function and evaluate the possible risks, as well as to realize that their actions in FB leave digital "traces" even if they are deleted. This indicates formal perceptions reverse. Although students supported their responsibility to protect themselves and other users within FB, it is revealed that they didn't have the required knowledge. Nevertheless, after the course completion, a great number of them had managed more strictly their profile visibility and FB privacy settings, while their uncertainty about the anti-spyware software usefulness was decreased. Though the positive impact of our educational intervention was highlighted through these shifts, the necessity for the adoption of certain technical measures was also revealed.

Furthermore, considering that the majority of the students supported that legislation can protect their privacy, despite their recorded relative acquaintance with current legislation, educational material should include more targeted information regarding this issue in the future. Specifically, educational material should include the new General Data Protection Regulation (GDPR), and the Greek legislation's harmonization to this, while a specialized lecture should focus on users' rights, such as right to access, right to be forgotten and erasure data right, as well as on SNS's responsibility for data protection, according to current national and European legislation. Additionally, students' evaluation regarding the intervention pointed out that they became more familiar with SNSs' operation and utility within different socio-economic environments, acknowledging benefits as well as risks both in a theoretical and practical aspect. It is also especially encouraging that students declared by the end of the course more conscious and aware when interacting and disclose personal information within SNSs. Therefore, in contrast to previous literature findings, our educational intervention is shown to have a significant impact on students' attitude and behavior, increasing both privacy awareness and concerns through realized risks in SNSs and confronting them by the adoption of protective privacy behaviors and technical protection strategies.

On the other hand, the acknowledged limitations of our study, with reference to a) the relevant small sample to which our intervention was addressed, b) the specific age group -*that already had a shaped system of perceptions, values and actions*- to which our sample belonged, c) the lack of a specialized lecture on GPDR and d) the fact that Phase II interview took place right after lectures completion, not allowing to explore whether the impact of the intervention would last or come up latter in time, as already underlined in literature (Vanderhoven et al., 2016), provides a foundation for further research on this area to be elaborated.

Future educational interventions on digital literacy enhancement regarding SNSs should be long-term oriented, as the results of the current intervention were more encouraging than those of short-term and should explore impacts on awareness and behavior not just after the completion of intervention but over a period of time. Furthermore, educational packages to be used should cover knowledge and skills gaps resulting from previous education, regardless variables as FB intensity usage. These packages should also emphasize on material regarding current legislation, companies' access to personal information as well as indirect information disclosure, while investigating at individual level perceptions on information sensitivity in relation to social norms and personal privacy needs. Finally, beyond the habitus and students' general knowledge, more other factors regarding their attitudes and behavior shifts -mainly at personal level- should be explored during the future educational interventions, such as personality traits which have a significant impact on human behavior.

6 References

Acquisti, A. and Gross, R. (2006), 'Imagined communities: Awareness, information sharing, and privacy on The Facebook'' in Danezis, G. and Golle, P. (eds), *Proceedings of the 6th Workshop on Privacy Enhancing Technologies (PET '06), LNCS*, vol. 4258, Springer Heidelberg, pp. 36-58.

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015), 'Privacy and human behavior in the age of information', *Science*, Vol. 347 No. 6221, pp. 509-514.

Arnett, J.J. (2000), 'Emerging adulthood: A theory of development from the late teens through the twenties', *American Psychologist*, Vol. 55, pp. 469–480.

Baek, Y.M., Kim, E. and Bae, Y. (2014), 'My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns', *Computers in Human Behavior*, Vol. 31, pp. 48–56.

Bargh, J.A. and McKenna, K. (2004), 'The Internet and social life', *Annual Review of Psychology*, Vol. 55, pp. 573–590.

Barnes, S.B. (2006), 'A privacy paradox: social networking in the United States', *First Monday*, Vol. 11 No. 9, available at : http://firstmonday.org/article/view/1394/1312_2 [Accessed February 2017]

Bartsch, M. and Dienlin, T. (2016), 'Control your Facebook: An analysis of online privacy literacy', *Computers in Human Behavior*, Vol. 56, pp. 147-154.

Bazarova, N.N. and Choi, Y. H. (2014), 'Self-disclosure in social media: Extending the functional approach to self-disclosure motivations and characteristics on social network sites', *Journal of Communication*, Vol. 64, pp. 635-657.

Benson, V., Saridakis, G. and Tennakoon, H. (2015), 'Information disclosure of social media users. Does control over personal information, user awareness and security notices matter?', *Information Technology & People*, Vol. 28 No. 3, pp. 426-441.

Bertot, J.C., Jaeger, P.T. and Grimes, J.M. (2010), 'Using ICTs to create a culture of transparency: e-government and social media as openness and anti-corruption tools for societies', *Government Information Quarterly*, Vol. 27 No. 3, pp. 264-271.

Bertot, J.C., Jaeger, P.T. and Hansen, D. (2012), 'The impact of polices on government social media use: issues, challenges, and recommendations, *Government Information Quarterly*, Vol. 29 No. 1, pp. 30-40.

Brandimarte, L., Acquisti, A. and Loewenstein, G. (2012), 'Misplaced Confidences: Privacy and the Control Paradox', *Social Psychological and Personality Science*, Vol. 4 No. 3, pp. 340-347.

Brandtzæg, P.B., Lüders, M. and Skjetne, J.H. (2010), 'Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites', *International Journal of Human-Computer Interaction*, Vol. 26, pp. 1006–1030.

Bourdieu, P. (1977), *Outline of a Theory of Practice*, Cambridge University Press, UK.

boyd, d. (2014), 'What does the Facebook experiment teach us?', *The Message*, available at: https://medium.com/message/what-does-the-facebook-experiment-teach-us-c858c08e287f#.tuxom8nw4 [Accessed February 2017].

boyd, D. and Hargittai, E. (2010), 'Facebook privacy settings: Who cares?, *First Monday*, Vol. 15 No.8., available at: http://journals.uic.edu/ojs/index.php/fm/article/view/3086/2589 [Accessed August 2018]

boyd, d. and Heer, J. (2006), 'Profiles as Conversation: Networked Identity Performance on Friendster' in *Proceedings of the Hawai'i International Conference on System Sciences (HICSS-39), Persistent Conversation Track*, IEEE Computer Society, Kauai, HI.

Bryant, E.M., Marmo, J. and Ramirez, A.Jr. (2011), 'A functional approach to social networking sites' in Wright, K.B. and Webb, L.M (Eds.), *Computer-mediated communication in personal relationships*, Peter Lang, New York, pp. 3-20.

Buschel, I., Mehdi, R., Cammilleri,A., Marzouki, Y. and Elger, B. (2014), 'Protecting Human Health and Security in Digital Europe: How to Deal with the ''Privacy Paradox''?', *Sci. Eng. Ethics*, Vol. 20, pp. 639–658.

Chen, R. (2013), 'Living a private life in public social networks: An exploration of member self-disclosure', *Decision Support System*, Vol. 55, pp. 661–668.

Cheung, C.M.K., Chiu, P-Y. and Lee, M.K.O. (2011), 'Online social networks: Why do students use Facebook?', *Computers in Human Behavior*, Vol. 27 No. 4, pp. 1337–1343.

Cheung, C., Lee, Z.W.Y. and Chan, T.K.H. (2015), 'Self-disclosure in social networking sites', Internet Research, Vol. 25 No. 2, pp. 279 – 299.

Conger, S., Pratt, J.H. and Loch, K.D. (2013), 'Personal information privacy and emerging technologies', *Information Systems Journal*, Vol. 23 No. 5, pp. 401-417.

Costello, C.R., McNiel, D.E. and Binder, R.L. (2016), 'Adolescents and Social Media: Privacy, Brain Development, and the Law', *J. Am. Acad. Psychiatry Law*, Vol. 44, pp. 313–21.

Debatin, B., Lovejoy, J.P., Horn, A.K. and Hughes, B.N. (2009), 'Facebook and online privacy: attitudes, behaviors, and unintended consequences', *Journal of Computer-Mediated Communication*, Vol. 15, pp. 83-108.

Del Rey, R., Casas, J.A. and Ortega, R. (2012), 'The ConRed Program, an Evidence based Practice', *Communicar- Scientific Journal of Media Education*, Vol. 39 No. XX, pp. 129-137.

Dienlin, T. and Trepte, S. (2015), 'Putting the Social (Psychology) into Social Media Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors', *Eur. J. Soc. Psychol*., Vol. 45, pp. 285–297.

Duran, R.L., Yousman, B., Walsh, K.M. and Longshore, M.A. (2008), 'Holistic Media Education: An Assessment of the Effectiveness of a College Course in Media Literacy', *Communication Quarterly*, Vol. 56 No. 1, pp. 49–68.

Dwyer, C., Hiltz, S. and Passerini K. (2007), 'Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace' in *Proceedings of 13th Americas Conference on Information Systems, AMCIS 2007*, ACM, Keystone, Colorado, USA.

Ellison, N.B., Steinfield, C. and Lampe, C. (2007), 'The benefits of Facebook ''friends'': Social capital and college students' use of online social network sites', *Journal of Computer-Mediated Communication*, Vol. 12 No. 4, pp. 1143–1168.

Ellison, N., Vitak, J., Steinfield, C., Gray, R. and Lampe, C. (2011), 'Negotiating privacy concerns and social capital needs in a social media environment' in Trepte, S. and Reinecke, L. (Eds.), *Privacy online: Perspectives on privacy and self- disclosure in the social web*, Springer, Berlin, Germany, pp.19-32.

European Commission (2012a), European Strategy for a Better Internet for Children, COM (2012) 196 final, Brussels, May 2, available at: file:///C:/Users/user1/Downloads/Communication.pdf [Accessed February 2017].

European Commission (2012b), *Joint Declaration between the Department of Homeland Security and the European Commission*, London, November 20, available at: https://thetyee.ca/Documents/2012/11/20/DepartmentofHomelandSecurityandtheEuropeanCommission-JointDeclaration.pdf [Accessed February 2017].

Feng, Y. and Xie, W. (2014), 'Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy- protecting behaviors', *Computers in Human Behavior*, Vol. 33, pp. 153–162.

Gibbs, J.L., Ellison, N.B. and Lai, C-H. (2011), 'First comes love, then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating', *Communication Research*, Vol. 38 No. 1, pp. 70–100.

Greek Ministry of Education, Research and Religious Affairs (2016a), *Curriculum and instructions for teaching "Information and Communication Technologies" in Primary Education during the school year 2016-17*, Athens, December 28, available at: https://app.box.com/s/kwepcz32fe7nu03b73xun3t0tgobwqts (in greek) [Accessed February 2017].

Greek Ministry of Education, Research and Religious Affairs (2016b), *Instructions for teaching Informatics in Secondary Education during the school year 2016-17*, Athens, September 15, available at: https://app.box.com/s/ey2r6cy4y5d4ffdu2jkor80wmj7m1l60 (in greek) [Accessed February 2017].

Gross, R. and Acquisti, A. (2005), 'Information revelation and privacy in online social networks' in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, ACM, Alexandria, VA, USA, pp. 71-80.

Hargittai, E. (2009), 'An update on survey measures of web-oriented digital literacy', *Social Science Computer Review*, Vol. 27 No. 1, pp. 130–137.

Hoadley, C.M., Xu, H., Lee, J.J. and Rosson, M.B. (2010), 'Privacy as information access and illusory control: The case of the Facebook news feed privacy outcry', *Electronic Commerce Research and Applications*, Vol. 9 No. 1, pp. 50−60.

Johnson, M., Egelman S. and Bellovin, St. M. (2012), 'Facebook and Privacy: It's Complicated' in *Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS'12*, article 9, ACM, Washington, USA, pp. 1-15.

Kim, J. and Lee, J.R. (2011), 'The Facebook paths to happiness: effects of the number of Facebook friends and self-presentation on subjective wellbeing', *CyberPsychology, Behavior and Social Networking*, Vol. 14, pp. 359–364.

Klein, W.M. and Kunda, Z. (1994), 'Exaggerated self-assessments and the preference for controllable risks', *Organizational Behavior and Human Decision Processes*, Vol. 59, pp. 410-427.

Kramer, N.C. and Haferkamp, N. (2011), 'Online Self-Presentation: Balancing Privacy Concerns and Impression Construction on Social Networking Sites' In Trepte, S. and Reinecke, L. (Eds.), *Privacy online: Perspectives on privacy and self- disclosure in the social web*, Springer, Berlin, Germany, pp. 127-141.

Krasnova, H., Spiekermann, S., Koroleva, K. and Hildebrand, T. (2010), 'Online social networks: why we disclose', *Journal of Information Technology*, Vol. 25, pp. 109–125.

Külcü, Ö. and Henkoğlu, T. (2014), 'Privacy in social networks: An analysis of Facebook', *International Journal of Information Management*, Vol. 34 No. 6, pp.761-769.

Lawler, J.P. and Molluzzo, J.C. (2010), 'A study of the perceptions of students on privacy and security on social networking sites (SNS), on the internet', *Journal of Information Systems Applied Research*, Vol. 3 No. 12, pp.3-18.

Lee, K.T., Noh, M.J. and Koo, D.M. (2013), 'Lonely people are no longer lonely on social networking sites: The mediating role of self-disclosure and social support', *Cyberpsychology, Behavior and Social Networking*, Vol. 16 No. 6, pp. 413-418.

Livingston, S. (2008), 'Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression', *New Media & Society*, Vol. 10 No. 3, pp. 393–411.

Livingstone, S. and Bulger, M.E. (2013), *A global agenda for children's rights in the digital age. Recommendations for developing UNICEF's research strategy*, LSE, London, UK.

Livingstone, S., Haddon, L., Görzig, A. and Olafsson, K. (2011), *Risks and Safety on the Internet: The Perspective of European Children. Full Findings*, LSE- EU Kids Online, London, UK.

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011, November). Analyzing facebook privacy settings: user expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference,* (pp. 61-70). ACM.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), 'Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model', *Information Systems Research*, Vol. 15 No. 4, pp. 336-355.

Marino, Cl., Vieno, A., Pastore, M., Albery, I., Frings, D. and Spada, M.M. (2016), 'Modeling the contribution of personality, social identity and social norms to problematic Facebook use in adolescents', *Addictive Behaviors*, Vol. 63, pp. 51–56.

Martens, H. (2010), 'Evaluating Media Literacy Education: Concepts, Theories and Future Directions', *The Journal of Media Literacy Education*, Vol. 2 No. 1, pp. 1–22.

Marwick, A. E. and boyd, D. (2014), 'Networked privacy: How teenagers negotiate context in social media', *New media & Society*, Vol. 16 No. 7, pp. 1051-1067.

Marwick, A.E., Murgia-Diaz, D. and Palfrey, J.G. (2010), *Youth, Privacy and Reputation (Literature Review),* Social Science Research Network, Rochester, NY.

Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D. and Torres, N. (2012), *Global survey on Internet privacy and freedom of expression*, Unesco Publishing, France.

Mishna, F., Cook, C., Saini, M., Wu, M-J. and MacFadden, R. (2010), 'Interventions to prevent and reduce cyber abuse of youth: A systematic review', *Research on Social Work Practice*, Vol. 21 No. 1, pp. 5–14.

Moll, R., Pieschl, St.and Bromme, R. (2014), 'Competent or clueless? Users' knowledge and misconceptions about their online privacy management', *Computers in Human Behavior*, Vol. 41, pp. 212-219.

Nguyen, M., Bin, Y.S. and Campbell, A. (2012), 'Comparing online and offline self-disclosure: A systematic review', *Cyberpsychology, Behavior and Social Networking*, Vol. 15 No. 2, pp. 103–111.

Nordgren, L.F., Van Der Pligt J. and Van Harreveld, F. (2007), 'Unpacking perceived control in risk perception: The mediating role of anticipated regret', *Journal of Behavioral Decision Making*, Vol. 20 No. 5, pp. 533-544.

Norris, C. (2003), 'From personal to digital: CCTV, the panopticon and the technological mediation of suspicion and social control' in Lyon, D. (ed.), *Surveillance and Social Sorting: Privacy Risk and Automated Discrimination*, Routledge, London, pp. 241-281.

O' Neil, D. (2001), 'Analysis of Internet Users' Level of Online Privacy Concerns', *Social Science Computer Review*, Vol. 19 No. 1, pp. 17-31.

Papacharissi Z. (ed.) (2011), *A networked self: Identity, community, and culture on social network sites*, Routledge, New York, USA.

Park, Y.J. (2011), 'Digital literacy and privacy behavior online', *Communication Research*, Vol. 40 No. 2, pp. 215–236.

Park, Y.J. and Jang, S.M. (2014), 'Understanding privacy knowledge and skill in mobile communication', *Computers in Human Behavior*, Vol. 38, pp. 296–303.

Pempek, T.A., Yermolayeva, Y.A. and Yermolayeva, S.L. (2009), 'College students' social networking experiences on Facebook', *Journal of Applied Developmental Psychology*, Vol. 30, pp. 227–238.

Posey, C., Lowry, P.B., Roberts, T.L. and Ellis, T.S. (2010), 'Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities', *European Journal of Information Systems*, Vol. 19 No. 2, pp. 181-195.

Prensky, M. (2001), 'Digital Natives, Digital Immigrants', *On the Horizon*, Vol. 9, pp. 1-6.

Ragnedda, M. (2011), 'Social control and surveillance in the society of consumers', *Int. J. Sociol. Anthropol.,* Vol. 3 No. 6, pp. 180–188.

Rains, S.A. and Brunner, S.R. (2015), 'The Outcomes of Broadcasting Self-Disclosure Using New Communication Technologies Responses to Disclosure Vary Across One's Social Network', *Communication Research*, pp. 1-29. Doi: 10.1177/0093650215598836

Raynes-Goldie, K. (2010), 'Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook', *First Monday*, Vol. 15 No. 1, available at: http://firstmonday.org/article/view/2775/2432 [Accessed February 2017].

Sheehan, K.B. (2002), 'Toward a typology of Internet users and online privacy concerns', *The Information Society*, Vol. 18, pp. 21–32.

Shoor, E. A. (2014), 'Narrowing the right to be forgotten: why the European Union needs to amend the proposed data protection regulation', *Brooklyn Journal of International Law,* Vol. 39 No. 1, pp. 487-519.

Sideri, M., Kitsiou, A., Kalloniatis, C., & Gritzalis. S. (2015), 'Privacy and Facebook Universities Students' Communities for Confessions and Secrets: The Greek Case', in Katsikas, S. & Sideridis, A. (eds) *Proceedings of the 6th International Conference on E-Democracy–Citizen Rights in the World of the New Computing Paradigms*, Springer International Publishing, Athens, Greece, pp. 77-94.

Sideri, M., Kitsiou, A., Tsortzaki, E., Kalloniatis, C. & Gritzalis, S. (2017), "I have learned that I must think twice before…". An educational intervention for enhancing students' privacy awareness in Facebook. In : S. Katsikas & V. Zorkadis, (eds) Proceedings of the 7th International Conference on E-Democracy–Privacy-Preserving, Secure, Intelligent E-Government Systems, December 2017, Athens, Greece: Springer International Publishing, pp. 79-94.

Smith, H.J., Dinev, T. and Xu, H. (2011), 'Information privacy research: an interdisciplinary review', *MIS Quarterly*, Vol. 35 No. 4, pp. 989-1015.

Spiliotopoulos, T. and Oakley, I. (2013), 'Understanding motivations for Facebook use: Usage metrics, network structure, and privacy' in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Paris, France, pp. 3287-3296.

Steijn, W.M.P. (2014), *Developing a sense of privacy: An investigation into privacy appreciation among young and older individuals in the context of social network sites*, Tilburg Institute of Law Technology and Society, Tilburg, available at https://pure.uvt.nl/ws/files/7737309/Steijn_Developing_05_09_2014_emb_tot_06_09_2015.pdf [Accessed February 2017].

Steinfield, C., Ellison, N., Lampe, C. and Vitak, J. (2012), 'Online social network sites and the concept of social capital' in Lee, F. L., Leung, L., Qiu, J. S. and Chu, D. (eds.), *Frontiers in New Media Research*, Routledge, New York, USA, pp. 115-131.

Steinke, J., Lapinski, M.K., Crocker, N., Zietsman-Thomas, A., Williams, Y., Evergreen, S.H. and Kuchibhotla, S. (2007), 'Assessing media influences on middle school–aged children's perceptions of women in science using the Draw-A-Scientist Test (DAST)', *Science Communication*, Vol. 29 No. 1, pp. 35–64.

Stutzman, F., Gross, R. and Acquisti, A. (2013), 'Silent listeners: The evolution of privacy and disclosure on facebook', *Journal of privacy and confidentiality*, Vol. 4 No. 2, pp. 7-41.

Stutzman, F., Vitak, J., Ellison, N.B., Gray, R. and Lampe, C. (2012), 'Privacy in Interaction: Exploring Disclosure and Social Capital in Facebook' in *Proceedings of the Sixth International Conference on Weblogs and Social Media*, AAAI org, Dublin, Ireland, pp. 330-337.

Taddicken, M. (2014), 'The 'Privacy Paradox in the Social Web: The Impact of Privacy Concerns, Individual Characteristics and the Perceived Social Relevance on Different Forms of Self-Disclosure', *Journal of Computer-Mediated Communication*, Vol. 19 No. 2, pp. 248-273.

Taddicken, M. and Jers, C. (2011), 'The uses of privacy online: trading a loss of privacy for social web gratifications?' in Trepte, S. and Reinecke, L. (Eds.), *Privacy online: Perspectives on privacy and self- disclosure in the social web*, Springer, Berlin, Germany, pp. 143-158.

Taneja, A., Vitrano, J. and Gengo, N.J. (2014), 'Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation', *Computers in Human Behavior*, Vol. 38, pp. 159-173.

Tayie, S., Pathak-Shelat, M. and Hirsjarvi, I. (2012), ' Young People's Interaction with Media in Egypt, India, Finland, Argentina and Kenya', *Communicar- Scientific Journal of Media Education*, Vol. 39 No. XX, pp. 53-62.

Thesis., A. (2014), 'The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data', *Wake Forest Law Review*, Vol. 49,pp. 433-484.

Trepte, S. and Reinecke, L. (2013), 'The reciprocal effects of social network site use and the disposition for self-disclosure: A longitudinal study', *Computers in Human Behavior*, Vol. 29 No. 3, pp. 1102-1112.

Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A. and Lind, F. (2015), 'Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS)' in Gutwirth, S., Leenes, R., de Hert, P. (Eds.), *Reforming European data protection law*, Springer, Heidelberg, Germany, pp. 333–365.

Tufekci, Z. (2012), 'Facebook, youth and privacy in networked publics' in *Proceedings of the Sixth International Conference on Weblogs and Social Media,* AAAI org, Ireland, Dublin, pp. 338-345.

UNESCO (2003), *The Prague Declaration "Towards an Information Society "*, Praque, September 20—23, available at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/PragueDeclaration.pdf [Accessed February 2017].

Utz, S. and Kramer, N. (2009), 'The privacy paradox on social network sites revisited: The role of individual characteristics and group norms', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, Vol. 3 No. 2, available at: http://www.cyberpsychology.eu/view.php?cisloclanku=20091110011 [Accessed February 2017].

Van den Broeck, E., Poels, K. and Walrave, M. (2015), 'Older and Wiser? Facebook Use, Privacy Concern, and Privacy Protection in the Life Stages of Emerging, Young, and Middle Adulthood', *Social Media and Society*, July-Dec., pp. 1 –11.

Vanderhoven, E., Schellens, T. and Valcke, M. (2013), 'Exploring the Usefulness of School Education about Risks on Social Network Sites: A Survey Study', *Journal of Media Literacy Education*, Vol. 5 No. 1, pp. 285-294.

Vanderhoven, E., Schellens, T. and Valcke, M. (2014), 'Educating teens about the risks on Social Network Sites. An intervention study in Secondary Education', *Communicar - Scientific Journal of Media Education*, Vol. 43 No. XXII, pp. 123-131.

Vanderhoven, E., Schellens, T., Vanderlinde R. and Valcke, M. (2016), 'Developing educational materials about risks on social network sites: a design-based research approach', *Education Tech Research Dev*, Vol. 64, pp. 459–480.

Walton, S. C. and Rice, R.E. (2013), 'Mediated disclosure on Twitter: The roles of gender and identity in boundary impermeability, valence, disclosure, and stage', *Computers in Human Behavior*, Vol. 29, pp. 1465-1474.

Williams, D. (2006), 'On and off the 'net: Scales for social capital in an online era', *Journal of Computer-Mediated Communication*, Vol. 11 No. 2, pp. 593–628.

Zhou, T. (2011), 'Understanding online community user participation: a social influence perspective', *Internet Research*, Vol. 21 No. 1, pp. 67-81.

Ziegele, M. and Quiring, O. (2011), 'Privacy in Social Network Sites' in Trepte, S. and Reinecke, L. (Eds.), *Privacy online: Perspectives on privacy and self- disclosure in the social web*, Springer, Berlin, Germany, pp. 175-189.