"I Have Learned that I Must Think Twice Before…". An Educational Intervention for Enhancing Students' Privacy Awareness in Facebook

Maria Sideri[1], Angeliki 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, 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, 83200 Samos, Greece
{etzortzaki,sgritz}@aegean.gr

Abstract. Social Network Sites have doubtless become part of our lives, facilitating communication and interaction between social actors. Within this frame users disclose personal information for several reasons while at the same time they express privacy concerns. "Privacy Paradox" reveals that despite privacy concerns, users, most of the times, fail to protect their privacy within SNSs, putting thus themselves and other users to risk. In this respect, several researches have shown that users' privacy awareness increase is of major importance, 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 educational intervention centered on a semester course of a Greek University, provides encouraging findings regarding students' privacy awareness enhancement.

Keywords: Social network sites · Facebook · Privacy concerns · Privacy awareness · Educational intervention · Semester course

1 Introduction

Social Network Sites (SNSs) are currently the most dynamically developing personal networking tool [1]. Their descriptive nature creates intimate feelings, which encourage information flow within them [2]. In this frame, users voluntarily provide personal information and/ or carelessly consent to its collection, while at the same time they raise anxieties about their privacy and the security of their information. The interrelation between privacy on SNSs and information disclosure "*is characterized by a constant tension between confidentiality and transparency*" [3] (p. 642). The Privacy Paradox [4] eventually results from a conflict situation between people's fear and anxiety of being observable, supervised and vulnerable because of personal information disclosed and their disclosure behavior in SNSs. To address that, beyond legislation and providers'

S.K. Katsikas and V. Zorkadis (Eds.): E-Democracy 2017, CCIS 792, pp. 79–94, 2017.
https://doi.org/10.1007/978-3-319-71117-1_6

techniques for privacy protection, users' privacy awareness increase and protective behavior adoption has been underlined of major importance. Privacy literacy is thus crucial in order for online privacy to be strengthened [5]. In this frame, educational interventions providing knowledge and skills on privacy management are expected to have a positive effect on users' behavior, altering existing disclosure practices.

This paper refers to an innovative educational intervention to enhance Greek University students' awareness providing insight to possible alteration of their privacy concerns and privacy management in Facebook. The intervention took place during the semester course entitled "Social Media: Identity, Communities and Application Fields", offered by the Department of Cultural Technology and Communication of the University of the Aegean. The paper is organized as follows. In Sect. 2, related work which focuses on digital literacy and educational interventions for enhancing users' knowledge and skills is presented. Section 3 refers to methodology applied, presenting research question and explicating study's design and the research stages followed. Section 4 presents the results of the research and discusses findings, while Sect. 5 concludes the paper and raises future research directions.

2 Related Work on Previous Educational Interventions

Researchers trying to interpret human behavior in SNSs investigate the factors that affect users to disclose personal information despite their stated privacy concerns. In this frame, information control, awareness level and risk perception are important to understand people's failure to transform their concerns into privacy protective behavior [6]. Digital literacy has been shown to have a positive effect on the protection of online privacy [7] aiming to enhance users' awareness about the extent of their knowledge [8] and to help them to accurately assess online risks [9] especially those arising from information disclosure. Trepte et al. [10] argue that online privacy literacy may be defined as a combination of declarative knowledge (knowledge about technical aspects of information protection, related with laws and directives) and procedural knowledge (ability to use strategies for individual privacy regulation and information protection). In this frame, educational campaigns are of major importance since they are expected to improve users' knowledge and provide skills to combat cyber threats and consequently reduce the possibilities of being attacked [11].

Digital literacy is indicated as basic life –skill that should be included in the education system from an early age [12]. Within this context, Taneja et al. [13] underline the obligation of schools, colleges and public libraries to develop educational interventions "*to reinforce individuals' beliefs related to information resource safety, information resource vulnerability, privacy concern, threat severity, privacy intrusion… and intrinsic cost associated with the use of privacy controls*" (p. 172). Especially, in the frame of education, at all levels, educators and teachers should launch educational programs in order for young people to modify the way they perceive their social context [14] and to raise their awareness [15].

Although the issue of online safety has been implemented in education, the results coming up from educational programs need further attention. Even though there is a

huge number of researches focusing on variables affecting users' awareness, researches focusing on the role and impact of school education on privacy attitudes and behavior on SNSs are relatively recent and focus mostly on school students, Vanderhoven et al. [15] argue that the attention given by school education to privacy attitudes and safe behavior is rather incidental, since these issues are not integrated in a course or in the curriculum. Furthermore, most of the developed educational packages about safety and security mostly focus on Internet risks in general [16], do not tackle with SNSs' specific risks and are not theoretically grounded [17] since few of them have been evaluated empirically [16]. This leads to a lack of educational lines that should be taken into consideration when designing such programs [18].

Referring to the outcomes of the educational packages that have been evaluated, Vanderhoven et al. [17] and Mishna et al. [19] argue that in cases when raising awareness and knowledge increase were observed, they were not followed though by risky behavior decrease which constitutes the ultimate goal of the intervention. This is consistent with the argument that media literacy education increases knowledge about the specific topic of the course, although changes in attitude and behavior usually may not come up [20]. The inconsistency between expected and observed goals leads to the acknowledgment 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 [21].

Within this frame, Vanderhoven's et al. [16] study aimed to "*propose a list of validated theoretical design principles for future development of educational materials about risks on SNSs*" (p. 459). The research was addressed to teenagers of secondary education to measure possible change regarding awareness, attitude and behavior within SNSs focusing on three different categories of SNS risks; content, contact and commercial. The findings show a positive impact of the given courses on awareness. The course on content risks had a positive effect on awareness of both content and contact risks. The same was observed with reference to the course on contact risks, while the course on commercial risks had a positive effect on awareness of these risks only. Nevertheless, no impact on students' attitudes and a limited only impact on their behavior were revealed. Students that had attended the course on content risks had changed privacy settings and the content of their profile, the ones that had attended the course on contact risks had changed privacy settings and their personal information, while the ones having attended the course on commercial risks had changed privacy settings and account settings as well. Thus, the goal of behavior change was merely achieved [16, 17]. The authors attribute the non-impact on attitude and the limited impact on behavior to courses' duration (only an hour) and to peers influence as well, explaining that impact may be revealed later in time [17].

ConRed program [18] also focused on users' awareness enhancement aiming to reveal users' perceptions about the degree of control they exert over information they share, to introduce familiarity with safety and personal information protection mechanisms on Internet and social networks and to reduce risks as cyber-bullying, harassment and addiction to the Internet. The program was designed according to the principles of normative social behavior theory and was organized around the areas of (a) Internet and social networks; (b) benefits of Internet use and instrumental skills and (c) risks and

advice on usage. It was addressed to the whole education community under scope (students, teachers and families) and its results were positive referring to students' involvement reduce in cases of cyber-bullying, excessive use of Internet and the risk of addiction. The outcomes also revealed a greater awareness of the students with reference to learning and using strategies in order to increase their control over the information released as well as to keep uploaded information private.

3 Methodology

3.1 Question Raised

Though most students use SNSs daily, they are in their majority unaware of possible risks or ignore the results coming up from information disclosure and don't show up privacy protective behavior even in the cases they realize that their personal information may be accessed and used by others. Since online privacy literacy is crucial for users' privacy awareness increase [5], attention should be paid to educational interventions 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 [22, 23]. Though the adopted educational approach focuses on security issues regarding Internet usage in general, without addressing specifically the issue of privacy risks in SNSs, while in cases where educational interventions are oriented to these risks do not have long enough duration, as they are usually provided in one or two hours lessons.

In this regard, building up on previous literature and going beyond the short-term courses of Greek school education that focus on Internet risks, a major research question is raised concerning the effects of a long-term University-based educational intervention for enhancing students' privacy literacy regarding SNSs. To address that, our research aims at providing insight to possible alteration of Greek students' privacy concerns and privacy management in Facebook (FB), which derive from an innovative educational intervention during the semester course entitled "Social Media: Identity, Communities and Application Fields", offered by the Department of Cultural Technology and Communication of the University of the Aegean. This research extends previous researches addressed to school students (not in Greece) trying to investigate the outcomes of a new type of intervention that includes experimental learning activities being addressed to people that are expected to evaluate privacy significantly.

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. The syllabus of the course "Social Media: Identity, Communities and Application Fields" included the required sections, in which our intervention could be structured and applied. The group of students attending this course with the probable exception of those that have attended a special non-formal education course on social media is expected to have knowledge of

general scope with reference to social media 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 semester of the graduate program.

The course "Social Media: Identity, Communities and Application Fields" is provided in three stages. In the first, students are theoretically introduced to online social networking as a social phenomenon. In the second, issues such as the online presentation of digital self, the function of the online communities, the sense of belonging in an online group, the reputation and recognition in SNSs, possible costs as result of online behavior, privacy protection and privacy paradox as well are presented. Stage 3 addresses issues regarding the impact of social media on social life, referring to behaviors such as cyber-bulling or cyber-sex, social media usage in the fields of education, culture, employment, economy, politics, communities of fans or social movements as well as social media's effect in shaping public opinion. In the frame of our intervention, the topics of stage 2 and 3 were discussed in class, after the elaboration of the respective experiential learning activities.

In each of the three stages of our intervention, main instructions regarding both personal strategies and technical mechanisms were provided in order to enhance students' knowledge and technical skills for the protection of their personal information. 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. To evaluate the effects of this long-term educational intervention, a two-phase experimental study was conducted. The students enrolled in this 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. Basic prerequisite for participating in the study was having a FB account. From the fifty-four (54) enrolled students, twenty-three (23) of them volunteered to participate in our experimental research procedures.

3.3 Phase I-Instrumentation and 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, privacy risks, students' awareness and their strategies for privacy protection. Specifically, Phase I-interview schedule included the following five sections of close-ended questions on a 5-Point Likert scale:

1. Facebook Usage. This section 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 items of the latter were adopted from [24] Internet Social Capital Scale.

2. FB Profile and Privacy Settings management. This section of questions, aiming to explore students' usage of FB profile settings and FB privacy settings, included items

with reference to privacy settings' activation when creating the profile, privacy settings' change and profile's visibility.

3. FB Self-disclosure. This section comprises of two sub-sections also, concerning personal information that students disclose directly on their profile and information they disclose on posts or other activities.

4. FB Privacy concerns. The first sub-section includes items concerning the extent of worries to issues such as companies' access to students' personal information, personalized advertisements or phishing, while the second explores concerns regarding disclosure of sensitive personal information to unwanted or unknown audience.

5. FB Privacy risks, awareness and protection strategies. This section divided into three sub-sections aiming to explore students' perceptions regarding privacy risks, their privacy awareness, as well as the privacy strategies they follow in FB.

Additionally, a set of three items to address students' socio-demographic characteristics was included in the last part of the instrument.

3.4 Phase II-Instrumentation and Control Procedure

After the completion of the course's 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. The 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 sections focus on:

1. Facebook Usage. This section of dichotomous questions was designed to verify students' knowledge sources regarding FB usage.

2. FB Self-disclosure, FB Profile and Privacy Settings management. The six sub-sections of dichotomous questions aimed to examine the possible alteration of students' disclosed information and their privacy settings management. Sub-sections 1 and 2 focus on the addition or removal, respectively, of personal information while the third one includes items regarding possible changes in provided information, within the last three months. Sub-sections 4 and 5 explore possible alteration regarding the restriction or the extension of students' profile visibility, while sub-section 6 refers to alteration of students' privacy settings during the last three months and to the reasons they motivated them to change the settings.

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

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

5. Educational Intervention Evaluation. This 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.

To set-up our intervention efficiently a pre-test was administrated to three students, including both the structured interviews of Phase I and Phase II and the teaching material of the course. This procedure intended to address the issues of data collection and instruments reliability, as well as to identify the range of students' embedded knowledge, deriving from the educational material taught. To conduct the students' interviews advantageously and to increase their reliability, the interview schedule in both Phases was followed in the exact same order, in the exact same way for each one, without following up on the interviewees' answers in.

4 Results and Discussion

To evaluate the outcomes of our educational intervention regarding students' privacy awareness and behavior, Phase I and Phase II records were analyzed using quantitive and qualitive speech analysis and were compared.

4.1 Facebook Usage

Findings of Phase I indicate that most of the students (48%) had created a 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. FB intensity usage measures are 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.

Most 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. These findings are consistent with previous research [25] regarding students' motives for participating in FB. However, it is extremely noteworthy that findings regarding students' perceived social capital benefits within FB highlight some contradictories. Most of the students (57%) declared that relationships in FB are not real, while a great proportion of them (52%) were uncertain regarding the FB positive impact on the improvement of their relationships. This indicates 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 affected by other variables, such as privacy concerns.

As far as students' technical knowledge for the creation of their profile and FB functions is concerned, 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 on 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 mainly by themselves or through help offered by a friend. Furthermore, in Phase II, students admitted not having the required knowledge regarding all FB functions, while 83% of

them declared that their previous formal education had not contributed to the enhancement of this knowledge.

4.2 FB Profile and Privacy Settings Management

Findings of Phase I show that most of the students (74%) had their profile visible to all, while the rest of them, in equally ratios (8.5%), provided visibility to friends, selected friends or friends and their friends. An important shift concerning students' FB Profile management is recorded according to the findings of Phase II. Specifically, 65% of those who had their profile 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 Phase 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 using privacy settings [26] has been recorded as risky behavior. In Phase II, 57% of those who had not activated privacy settings declared that they had changed them within the last three months, a period coincident with the semester course, justifying this change in the context of obtaining more privacy protection within FB, as well as because of the attention they paid to the security notices that came up.

The above 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 and emphatically support previous work [15] as far as the necessity of education targeted on this issue is concerned.

4.3 FB Self-disclosure

Findings of Phase I indicate that the majority of students had used their actual personal information in their FB profiles. Specifically, according to the following Table 1, they used:

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. During Phase II, students were asked if they had removed any information from their FB profile within the last three months. 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 post address, and 4% birth date. This reveals a minor shift. As far as indirect information disclosure is concerned, both in Phase I and II, 35% of the students admitted sharing happy or unhappy moments, success or failure within FB, while posts regarding personal political beliefs seem to be avoided (74%). Additionally, students, in Phase I, declared (44%) that they usually tag other persons' names in their photos, while in Phase II, they stated that the specific practice is more than familiar to them (70%). Taking the above findings under consideration, it is indicated that special emphasis should have been given regarding indirect information disclosure practices as well as the sensitivity degree of information.

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 do have. Perceived control over personal information is crucial since it can lead either to a sense of security and thus to more information disclosure or to high privacy concerns generation and disclosure willingness decrease even in cases of lower risks resulting from disclosure [27]. Furthermore, 70% of the students in Phase II expressed their certainty that their shared information will not result in troubles in the future.

These findings indicate the advantages of our educational intervention, supporting [28] thesis 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

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, even though in Phase I most of the students (82%) were not at all concerned regarding companies' ability to access their personal information, in Phase II, this percentage was reduced to 74%. Since privacy concerns may burden the self-disclosure process [29], it is indicated that our educational intervention should be more focused on companies' access to personal information through SNSs.

After the completion of our educational intervention, students' anxiety centered on Phishing within FB was also recorded. Specifically, a notable shift has been recorded 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%). Findings, in Phase II, show a positive alteration only

regarding 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 [30], our educational intervention should have given special emphasis on that issue.

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

These findings indicate an explicit impact on students' privacy awareness deriving from our intervention while they also support previous work [31] regarding the usefulness of privacy control techniques that allow users to successfully manage privacy threats from unknown external audience.

4.5 FB Privacy Risks

During Phase I, most of the students (61%) declared that they didn't deal with any risk within FB, while in Phase II, 74% of the total 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, most of them (87%) understood that their previous perceptions were misguided.

Most of the students (83%), in Phase I, were not aware of the fact that FB, as a provider, gathers users' personal information. This finding supports previous work [32] 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 providers. Though, in Phase II, 87% of the students declared that had acknowledged this as a risk. In Phase II also, 83% of the students acknowledged that governments may have access to users' personal information through FB, while in Phase I only 61% of them shared this perception.

These findings show, supporting Chen's [9] 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

As far as control techniques related to the FB are concerned, all students stated in Phase I they acknowledged its technical functions. However, in Phase II, 69% of them demonstrated that they were aware of possible dangers deriving from FB technical characteristics that they didn't know before. This finding supports previous work [33], which indicates 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. 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%.

With reference to students' personal protection strategies, findings indicate that most of the students in Phase I supported that they themselves have to undertake 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 [18] that record the necessity for students to learn various strategies for augmenting their information control in SNSs. 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 this knowledge. 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.

4.7 Educational Intervention Evaluation

Our study was completed with students' evaluation concerning their perceived outcomes deriving from our educational intervention. Findings indicate that all students affirmed that they enhanced their knowledge and 96% of them affirmed that became aware not only of the benefits but also of the risks deriving from social media usage, both in a theoretical and practical aspect. One of the most important outcomes of the intervention concerns awareness enhancement. Most 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, most of the students (87%) declared that, after the semester course, they were more conscious of the practices that should adopt when acting in SNSs. This was recorded in several statements as "I have learned that I must think twice what might be hidden behind a profile or a post…". "I understood that Internet and its applications should be used with prudence" or "…I have also learned how to present myself without risking".

5 Conclusions

Digital literacy has been recorded as a prerequisite for online safety and has been included in the school curricula of the European countries. Though, as literature has shown [16, 17], online safety issue mostly focuses on Internet, ignoring SNSs specific features. The current research was addressed to a group of University students enrolled in the course titled "Social Media: Identity, Communities and Application Fields" offered by the Department of Cultural Technology and Communication of the University

of the Aegean. This semester course included the sections by which our educational intervention could be structured and applied. The intervention focused on enhancing students' knowledge about risks deriving from social media usage in order for their awareness to be increased and consequently privacy protective behavior to be adopted.

The contribution of our educational intervention, in comparison to previous, is centered on its duration, its target group and its context. In contrast to former short-term relevant interventions, it lasted 13 weeks and was addressed to Tertiary Education students, taking into account that such kind of educational programs should simultaneously emphasize on both positive aspects and risks in SNSs. From the beginning of the intervention we acknowledged that students, aged in their majority between 20–25 years old, acquire already –in comparison to younger users- a shaped system of dispositions, tendencies, perceptions and consequently social actions, which is outlined by the concept of "habitus" [34]. Habitus was thus expected to be a possible obstacle in changes of students' concepts or actions. Nevertheless, the embedding of new knowledge covering previous cognitive gaps was expected to have an impact on concepts and actions. Current research has also confirmed students' knowledge gaps concerning privacy issues and protective behavior resulting from students' previous education. These gaps that should be taken into consideration for the Greek school curricula design (primary and secondary education) were adequately covered. In contrast to previous research findings having revealed no impact of educational interventions on students' attitudes and only a limited impact on their behavior, our intervention is shown to have a significant impact on students' attitude, increasing both privacy awareness and concerns through acknowledging risks in SNSs and confronting them. Awareness increase led students to adopt privacy protective behavior either by using personal strategies or employing technical mechanisms.

The results of our research pointed out that most of students had created their profile by the age of 16 years old, having been FB users for at least 4 years. Since FB intensity usage is recorded, in previous researches, to have a positive impact on knowledge, students should have been rather familiar with FB functions, but they hadn't. The fact that, as students stated, previous formal education had not contributed to the increase of their knowledge, enhances previous literature regarding courses' focus on internet usage in general. These results point out the need for establishment of specific long-term educational measures that will reinforce students' digital literacy, regardless FB intensity usage, in order to cover knowledge gaps.

Concerning profile's visibility, findings point out a significant alteration in students' profile visibility management with regard to its restriction. The same shift is recorded with reference to students' management of privacy settings, deriving from their need to obtain more privacy protection within FB, while the necessity for the adoption of certain technical measures in this targeted training is also revealed.

Results highlighted that most of the students didn't remove disclosed information from their profiles within the three months of our intervention. Regarding indirect information disclosure, results point out that, before the semester course, about half of the students used to tag other persons' names in their photos, while no reverse behavior has been recorded after its completion. The above findings can be attributed to the fact that changes in attitude and behavior may come up later in time, as literature has already

recorded [16], or to habitus. Nevertheless, the need for ongoing monitoring of online behaviors is underlined.

Encouraging results by the educational intervention came up with reference to "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. Also, the majority of them expressed certainty of shared information not resulting in troubles in the future. The above findings clearly show that the intervention helped students to acknowledge risks and confront them.

Referring to privacy awareness, students' concerns regarding companies' access to their personal information were decreased a little, after the course, indicating the necessity for the educational material to be more focused on that issue. Phishing concerns on the contrary rose notably, while the ratio of students not concerned about other users' access to their thoughts and feelings reduced regarding only thoughts. The non-subversion of feelings disclosure practice can be seen in terms of social developmental goals or of habitus. It is indicated thus that emphasis should be placed during future educational interventions on outlining risks resulting from feelings' disclosure. Students' concerns regarding unwanted audience's knowledge about their location and activities reduced due to their profile's visibility restriction and the differentiated use of FB features. These adopted practices underline the accomplishment of privacy awareness enhancement goal.

Students' low awareness level resulting from their lack of knowledge regarding FB functions was confront helping them understand the key features of SNSs' function and evaluate possible risks deriving from their usage. Moreover, students realized that their actions in FB leave digital "traces" and that even if any action is deleted it can be found. This indicates formal perceptions reverse. The majority of the students also acknowledged that FB gathers users' personal information and understood that governments may also have access to their personal information through FB.

Furthermore, the results show that students' awareness to identify and adopt specific personal and technical protection strategies related to personal information disclosure behavior was enhanced. These findings combined with that of students decreased uncertainty about the anti-spyware software usefulness, highlight the impact of our intervention. 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, a great number of students had acquired knowledge and skills to support their protection.

Finally, awareness increase regarding the necessity to balance between their desire to interact with other people and protect their privacy is recorded by all students during the evaluation of the intervention and in this frame of reference it is especially encouraging that students declare more conscious when interacting in SNSs.

Limitations with reference to our research focus on the relevant small sample to which the intervention was addressed, even though sample's number constitutes about half of the students' enrolled in the course. Moreover, all participants belong to an age group that already has a shaped system of perceptions, values and actions. Even though knowledge is better embedded in older age groups comparing to younger, it isn't clear whether it can totally affect their actions since habitus alteration is a complicated process.

Nevertheless, it should be underlined that this age group (emerging adulthood) is likely to apply stricter privacy settings on SNS [26] -altering thus a formated action- and within this perspective awareness of the risks due to personal information disclosure constitutes a critical background. Finally, it should be noted that Phase II interview took place right after lectures' completion, due to several educational obligations that students had, thus not allowing to explore whether the impact of the intervention would last or results of the impact would come up latter in time, as already underlined in literature [16].

Future educational interventions on digital literacy enhancement regarding SNSs should be also 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 or age. They should also include material regarding legislation, companies' access to personal information and indirect information disclosure, while investigating at individual level perceptions on information sensitivity in relation to social norms and personal privacy needs.

References

1. Lin, K.Y., Lu, H.P.: Why people use social networking sites: an empirical study integrating network externalities and motivation theory. Comput. Hum. Behav. **27**(3), 1152–1161 (2011)
2. Pearson, E.: All the world wide web's a stage: the performance of identity in online social networks. First Monday **14**(3) (2009). http://firstmonday.org/article/view/2162/2127. Accessed Feb 2017
3. Buschel, I., Mehdi, R., Cammilleri, A., Marzouki, Y., Elger, B.: Protecting human health and security in digital Europe: how to deal with the "privacy paradox"? Sci. Eng. Ethics **20**, 639–658 (2014)
4. Dienlin, T., Trepte, S.: 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. **45**, 285–297 (2015)
5. Bartsch, M., Dienlin, T.: Control your Facebook: an analysis of online privacy literacy. Comput. Hum. Behav. **56**, 147–154 (2016)
6. Baek, Y.M.: Solving the privacy paradox: a counter-argument experimental approach. Comput. Hum. Behav. **38**, 33–42 (2014)
7. Park, Y.J.: Digital literacy and privacy behavior online. Commun. Res. **40**(2), 215–236 (2011)
8. Moll, R., Pieschl, S., Bromme, R.: Competent or clueless? Users' knowledge and misconceptions about their online privacy management. Comput. Hum. Behav. **41**, 212–219 (2014)
9. Chen, R.: Living a private life in public social networks: an exploration of member self-disclosure. Decis. Support Syst. **55**, 661–668 (2013)
10. Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A., Lind, F.: 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, pp. 333–365. Springer, Heidelberg (2015). https://doi.org/10.1007/978-94-017-9385-8_14
11. Marcolin, B.L., Compeau, D.R., Munro, M.C., Huff, S.L.: Assessing user competence: conceptualization and measurement. Inf. Syst. Res. **11**(1), 37–60 (2000)

12. Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D., Torres, N.: Global Survey on Internet Privacy and Freedom of Expression. Unesco Publishing, France (2012)
13. Taneja, A., Vitrano, J., Gengo, N.J.: Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: an empirical investigation. Comput. Hum. Behav. **38**, 159–173 (2014)
14. Marino, C., Vieno, A., Pastore, M., Albery, I., Frings, D., Spada, M.M.: Modeling the contribution of personality, social identity and social norms to problematic Facebook use in adolescents. Addict. Behav. **63**, 51–56 (2016)
15. Vanderhoven, E., Schellens, T., Valcke, M.: Exploring the usefulness of school education about risks on social network sites: a survey study. J. Media Liter. Educ. **5**(1), 285–294 (2013)
16. Vanderhoven, E., Schellens, T., Vanderlinde, R., Valcke, M.: Developing educational materials about risks on social network sites: a design based research approach. Educ. Tech. Res. Dev. **64**, 459–480 (2016)
17. Vanderhoven, E., Schellens, T., Valcke, M.: Educating teens about the risks on social network sites: an intervention study in secondary education. Communicar Sci. J. Media Educ. **43**(XXII), 123–131 (2014)
18. Del Rey, R., Casas, J.A., Ortega, R.: The ConRed program, an evidence based practice. Communicar Sci. J. Media Educ. **39**(XX), 129–137 (2012)
19. Mishna, F., Cook, C., Saini, M., Wu, M.-J., MacFadden, R.: Interventions to prevent and reduce cyber abuse of youth: a systematic review. Res. Soc. Work Pract. **21**(1), 5–14 (2010)
20. Steinke, J., Lapinski, M.K., Crocker, N., Zietsman-Thomas, A., Williams, Y., Evergreen, S.H., Kuchibhotla, S.: Assessing media influences on middle school–aged children's perceptions of women in science using the Draw-A-Scientist Test (DAST). Sci. Commun. **29**(1), 35–64 (2007)
21. Livingstone, S., Bulger, M.E.: A global agenda for children's rights in the digital age. Recommendations for developing UNICEF's research strategy. LSE, London (2013)
22. Greek Ministry of Education, Research and Religious Affairs. Curriculum and instructions for teaching "Information and Communication Technologies" in Primary Education during the school year 2016–17. https://app.box.com/s/kwepcz32fe7nu03b73xun3t0tgobwqts. (in greek)
23. Greek Ministry of Education, Research and Religious Affairs. Instructions for teaching Informatics in Secondary Education during the school year 2016–17. https://app.box.com/s/ey2r6cy4y5d4ffdu2jkor80wmj7m1l60. (in greek)
24. Williams, D.: On and off the'net: scales for social capital in an online era. J. Comput. Med. Commun. **11**(2), 593–628 (2006)
25. Krasnova, H., Spiekermann, S., Koroleva, K., Hildebrand, T.: Online social networks: why we disclose. J. Inf. Technol. **25**, 109–125 (2010)
26. Debatin, B., Lovejoy, J.P., Horn, A.K., Hughes, B.N.: Facebook and online privacy: attitudes, behaviors, and unintended consequences. J. Comput. Med. Commun. **15**, 83–108 (2009)
27. Brandimarte, L., Acquisti, A., Loewenstein, G.: Misplaced confidences: privacy and the control paradox. Soc. Psychol. Pers. Sci. **4**(3), 340–347 (2012)
28. Taddicken, M., Jers, C.: The uses of privacy online: trading a loss of privacy for social web gratifications? In: Trepte, S., Reinecke, L. (eds.) Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web, pp. 143–158. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21521-6_11
29. Stutzman, F., Gross, R., Acquisti, A.: Silent listeners: the evolution of privacy and disclosure on facebook. J. Priv. Confid. **4**(2), 7–41 (2013)

30. Sideri, M., Kitsiou, A., Kalloniatis, C., Gritzalis, S.: Privacy and facebook universities students' communities for confessions and secrets: the greek case. In: Katsikas, S.K., Sideridis, A.B. (eds.) e-Democracy 2015. CCIS, vol. 570, pp. 77–94. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-27164-4_6
31. Johnson, M., Egelman, S., Bellovin, S.M.: Facebook and privacy: it's complicated. In: Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS 2012), pp. 1–15. ACM, Washington (2012)
32. Lawler, J.P., Molluzzo, J.C.: A study of the perceptions of students on privacy and security on social networking sites (SNS), on the internet. J. Inf. Syst. Appl. Res. **3**(12), 3–18 (2010)
33. Nguyen, M., Bin, Y.S., Campbell, A.: Comparing online and offline self-disclosure: a systematic review. Cyberpsychol. Behav. Soc. Netw. **15**(2), 103–111 (2012)
34. Bourdieu, P.: Outline of a Theory of Practice. Cambridge University Press, Cambridge (1977)