IRIS AperTO

UNIVERSITÀ DEGLI STUDI DI TORINO

AperTO - Archivio Istituzionale Open Access dell'Università di Torino

A Social Network Simulation Game to Raise Awareness of Privacy among School Children

This is the author's manuscript

Original Citation:

Availability:

This version is available http://hdl.handle.net/2318/1681247 since 2020-04-26T14:24:28Z

Published version:

DOI:10.1109/TLT.2018.2881193

Terms of use:

Open Access

Anyone can freely access the full text of works made available as "Open Access". Works made available under a Creative Commons license can be used according to the terms and conditions of said license. Use of all other works requires consent of the right holder (author or publisher) if not exempted from copyright protection by the applicable law.

(Article begins on next page)

09 February 2025

A Social Network Simulation Game to Raise Awareness of Privacy among School Children

Livio Bioglio, Sara Capecchi, Federico Peiretti, Dennis Sayed, Antonella Torasso and Ruggero G. Pensa *

Abstract—In this paper, we address the problem of enhancing young people's awareness of the mechanisms involving privacy in online social networks by presenting an innovative approach based on gamification. In particular, we propose a web application that allows kids and teenagers to experience the typical dynamics of information spread through a realistic interactive simulation. Under the supervision of the teacher, the students are inserted in a small artificial social graph, and, through the different stages of game, they can post sentences with different levels of sensitivity, and "like" or share messages published by friends. At the end of game session, the application calculate multiple behavioral scores, that can be used by the teacher to raise the curiosity of the students and stimulate discussions. Moreover, a complete interactive report is generated to analyze every individual action of the terminated game sessions. Our educational tool has been employed within an extensive experimental study involving more than 450 kids and 22 teachers in seven Italian primary school institutes. The results show that our approach is stimulating and supports teachers in helping kids discover and recognize potential privacy risks in social network activities.

Index Terms—digital literacy, social media, privacy, school, educational support.

1 Introduction

The problem of user privacy in the so-called "Big Data Era" cannot be ignored, and online social network (OSN) providers have improved considerably the privacy protection tools featured by their web and mobile products. However, in OSN's the most powerful data protection "weapons" are the users themselves. In fact, social media (e.g., Facebook, Instagram, Twitter) are essentially human-generated logs that can be used to reconstruct life events and private facts of those users that carelessly disclose their personal information. According to several studies, however, the awareness of the importance of online privacy is still insufficiently widespread [1], [2], [3]. This problem involves both adults and minors, but the latters (mainly composed by the so-called "digital natives") are more affected by its consequences because of their vulnerability.

A recent survey [4] conducted by the IPSOS institute[1] for Save the Children (an international non-governmental organization that promotes children's rights, provides relief and helps support children in developing countries) showed that, in Italy, teenagers (aged 12-17, forming the so-called "Generation Z") are always online: they use Facebook (75%), WhatsApp (59%), Instagram (36%) and Twitter (29%), know quite well the rules that govern privacy in the Internet (51%), but they do not care that much (57%). In addition, they live virtual relations in chat rooms on their smartphone messaging applications, often with people they do not know directly (41%), almost one in four (24%) send messages, videos or pictures with sexual content to groups with unknown participants and one in three (33%) arranges to meet with someone known only through these groups. In recent years, several cyberbullying cases have garnered global attention on how much dangerous could be this behavior, in particular for kids and teenagers[2].

The main problem appears to be the poor perception that young people have of their own (and others') online privacy. Italian teenagers seem to ignore the mechanisms that regulate the spread of information on the Internet, especially in social networks; consequently they underestimate the potential diffusion of their thoughts, pictures and social actions when they are interconnected with the world. These numbers are favored by the more and more widespread use of mobile devices among the young people. Italians teenagers are early users of mobile devices: the average age in which they receive the first smartphone is 12 years and a half, and they learn to use it primarily by themselves (58%). The same IPSOS report shows that these digital devices could also be used actively for learning in the classroom. However, the use of smartphones in the classroom is largely prohibited: only 2% of teens surveyed admitted to having used them as part of a lesson.

To face the problem of unperceived online privacy issues, several activities have been proposed by governmental institutions jointly with schools. In particular, the Postal and Communications Police[3] has been organizing lectures in forms of frontal instruction to show the dangers of the Internet and how to face them. However, these activities are not specifically tailored on the problem of privacy in online social networks. Instead, they address general web security issues with the aim of protecting kids against cyberbulling and pedophilia issues. Moreover, they are conducted in a traditional teacher-centered form, while other advanced form of learning approaches (such as collaborative learning [5], active learning [6] and networked collaborative learning [7]) have been shown more effective for young pupils education.

* *L. Bioglio, S. Capecchi, F. Peiretti, D. Sayed and R.G. Pensa are with the Department of Computer Science, University of Torino I-10149 Torino, Italy.*
E-mail: ruggero.pensa@unito.it
- *A. Torasso is with Ministry of Education, Universities and Research, Italy.*
E-mail: antonella.torasso@istruzione.it

1. http://www.ipsos.it/
2. https://nobullying.com/six-unforgettable-cyber-bullying-cases/
3. http://www.commissariatodips.it/

In this paper we address the problem of enhancing privacy perception and awareness in online social network users by means of an innovative approach based on gamification. In particular, we propose *Social4School*[4], a web application that allows children and teenagers to experience the typical dynamics of information spread across an online social network through a realistic interactive simulation. Under the supervision of the teacher, the students use desktops or mobile devices (e.g., tablets) to join a dedicated game session. They are inserted in a small and local artificial social graph, and through the different stages of the game they can choose the sentences to publish, as well as "like" or share messages posted by friends. At the end, the game provides multiple scores for evaluating the user behavior: such scores can be used by the teacher for providing personalized suggestions to each student and for raising their curiosity. Moreover, a complete interactive report is generated to analyze every individual action of the terminated game sessions. The ultimate goal is to provide support for teachers to make children and young people aware of the mechanisms involving the diffusion of private information in online social networks.

Our approach has been validated in seven primary school complexes in the Piedmont regional area in Northern Italy. The experiment, which involved more than 450 kids and 22 teachers, has shown that our tool is a valid support for teachers to enhance kids' awareness on privacy issues related to the sharing of content in online social networks. Moreover, by means of a short questionnaire, we verified that the acquired knowledge is not limited to the specific scenario of our serious game. The results show that the improved awareness of the participants involves more general privacy aspects. Finally, we also surveyed the teachers who participated in our activities and acquired some important suggestions for future extensions of our educational project.

The remainder of the paper is organized as follows: Section 2 presents some related work; in Section 3 we present the dynamics of the game as implemented in our web application; we report the results of the experimental validation in Section 4; finally, Section 5 provides some concluding remarks and future work.

2 Related work

Privacy of individuals is being seriously threatened by the unrestrained success of online social networks, as shown by several psychological and computer science studies. For instance, the research project myPersonality [2] carried out at the University of Cambridge, has demonstrated that, by leveraging Facebook user's activity (such as "Likes" to posts or fan pages) it is possible to "guess" some very private traits of the user's personality. The same research team has recently launched Apply Magic Sauce[5], a web service that predicts users' psycho-demographic traits based on their digital footprints. According to another study, it is even possible to infer some user characteristics from the attributes of users who are part of the same communities [8]. Hence, privacy in online social networks is a major issue involving the rights and dignity of human beings and there has been increasing research interests about privacy protection methods for individuals that participate in them. The main research direction are essentially three: i) improving data protection by means of graph anonymization techniques using edge modification [9], [10], [11], randomization [12], [13], generalization [14], [15], differentially private mechanisms [16], [17] or secure access control techniques [18]; ii) improving user awareness by means of privacy risk metrics [19] or privacy settings optimization tools [20]; iii) improving user awareness by means of social games [21].

According to this literature analysis, it can be observed that, while data protection is a well explored research area, less attention has been given to the privacy risk of users caused by their information-sharing activities (e.g., posts, likes, shares). In fact, since disclosing information on the web is a voluntary activity, a common opinion is that users should care about their privacy and control it during their interaction with other social network users. Although multiple complex factors are involved in user privacy protection on social media [22], privacy controls for online social networking sites are not fully socially aware [23] and are barely utilized in practice. This statement is confirmed by [1], where it is shown that 36% of Facebook content is shared with the default privacy settings and exposed to more users than expected. According to another study, even restraining privacy settings are ineffective when the user is located within an unsafe network [24]. Privacy fatigue, (i.e., the tendency of online users to disclose greater information over time due to increasingly complex and less usable privacy controls) is another factor that has been recognized to play a significant role in favoring behaviors which endanger information privacy [25]. Thus, more effort should be done to educating people to recognize and prevent privacy issues in social media.

A very recent field of research proposes serious games to improve people's perception and awareness of their own and others' privacy. In [21], for instance, the authors present an online game, called *Friend Inspector*, that allows Facebook users to check their knowledge of the visibility of their shared personal items and provides recommendations on how to improve privacy settings. *Data Dealer*[6], instead, is an online game about collecting and selling personal data aiming at raising awareness about online privacy in a way that reminds some typical Facebook game. Similarly, RTS (Radio Télévision Suisse, the Swiss public broadcasting organization), provides *DATAK*[7], a serious game to raise awareness on issues related to the world of big data. It is intended for young people aged 15 years and older, letting them face and experience everyday situations, which have an impact on privacy and disclosure of personal data.

Although there are many evidences in the literature about benefits of the use of simulations and games for teaching and learning [26], [27], [28], at the best of our knowledge, there are no games specifically tailored for children and designed to be adopted as an educational tool to teach privacy at school. However, gamification has been extensively used in class education to address many different issues.

4. In Italian, the word "social", employed as a noun, stands for a generic social media platform.
5. http://applymagicsauce.com/
6. http://datadealer.com/
7. http://www.datak.ch/

In [29], the authors develop a multi-touch interactive game to assist primary school students in solving geographical puzzles. The authors of [30] investigate how a gamified learning approach influences science learning, achievement and motivation, through a context-aware mobile learning environment, and explain the effects on motivation and student learning. Gamification is also used in adult contexts, such as university courses and professional training courses. In [31], the authors analyze the achievements obtained by the introduction of gamification in a university course. Instead, in [32], the authors present an educational game development approach focused on the teaching of procedural knowledge in healthcare education. Finally, gamification has been investigated in conjunction with social networking in [33], where the authors present the results of testing both social networking and gamification in an undergraduate course, comparing them in terms their effect on students' academic achievement, participation and attitude.

3 A GAMIFIED SOCIAL NETWORKING EXPERIENCE

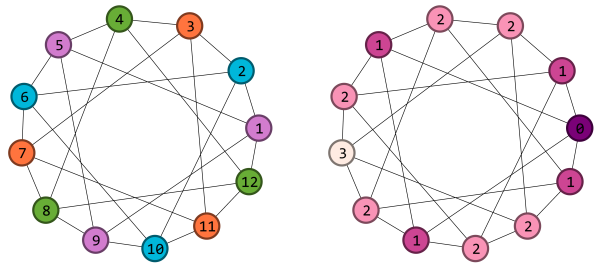
In this section we present the details of our serious game named *Social4School*. The goal of our game is to let young people experience the typical dynamics of an online social network in a simulated and controlled environment (a sort of *sandbox*). The teacher drives the simulation through her control panel, from which she can also monitor the activity of each participant. By discovering the phenomenon of information propagation in the social graph, users of our game enhance their perception of privacy issues related to online social networks and may improve their awareness about the protection of their own and others' personal data and facts. A set of behavioral scores, provided at the end of the simulation, ignite the curiosity of young people and help teachers organize their work during all subsequent classroom activities.

In the following, we first describe the dynamics of our serious game, then we address the computational details of the scores and present the functionalities provided by the teacher's control panel. Finally, we provide some details on the design methodology we adopted and on the implementation of the resulting web application.

3.1 Dynamics of the game

Before entering the details of our serious game, we provide some preliminaries and notations that we will use in the remainder of the paper. Each session of our game involves a set $U = \{u_1, \ldots, u_N\}$ of N participants (users) organized into a set $C = \{c_1, \ldots, c_K\}$ of $K < N$ disjoint groups such that each user belongs exactly to one group and each group contains at least one user.

Users in U are part of a social network. Without loss of generality, we assume that the link between two users is always reciprocal (if there is a link from u_i to u_j then there is also a link from u_j to u_i). Hence, the social network here is represented as an undirected graph. Given a pair of users $(u_i, u_j) \in U$, there exists an edge between u_i and u_j iif users u_i and u_j are connected by a friendship link. The social network is connected (the number of connected components is exactly one) and it is constructed as follows: there exists an edge between each pair of users belonging to the same group, and there exist some spurious edges between users belonging to different groups, called *bridge users*[8].



(a) An example of social graph generated within *Social4School*. Users in the same group are all connected together. Some groups are connected by spurious links involving their users.

(b) Node visibility in each reactive phase w.r.t. node 1. In the first reactive phase, only post of the first node's friends are visible. In the second reactive phase posts of all friends of node 1's friends become visible to node 1. In the third phase all remaining nodes are finally visible.

Fig. 1. An example of participant network (left) and visibility of its nodes w.r.t. a single node depending on the reactive phase number (right).

A schematic view of a friendship graph generated within our serious game is given in Fig. 1(a). Later we discuss on how we generate a graph with these features.

A set of M predefined posts (sentences), denoted as $P^k = \{p_1^k, \ldots, p_M^k\}$, is assigned to each group. A predefined score $score(p_m^k)$ is assigned to each post p_m^k: such score denotes the sensitivity level of the item w.r.t. privacy, from less sensitive (0) to most sensitive (5). As an example, the following sentence *"I like hamburgers and fries!"* is totally unsensitive, while *"Please call me at (555)123456."* may be considered as moderately sensitive as it contains a private phone number. Similarly, the sentence *"Mom seems very tired! She takes some strange pills."* is very sensitive as it provides some information about the health status of a family member. Note that the same scoring system can be applied on other kinds of social content, such as drawings, pictures or videos.

Users can perform three kinds of actions. A user $u_i \in c_k$ can post (aka publish) item p_m^k on her social profile, (notice that users can only choose the items assigned to their group), or, given an item p_m^k posted by user $u_j \in c_k$, she can like it or share it. For the sake of simplicity and brevity p_{im} will denote the item p_m^k posted by user u_i, and a_{ijm} will denote the item p_m^k posted by user u_j and liked or shared by user u_i.

The simulation of social interaction within *Social4School* works as described in Fig. 2. These game steps are synchronous, and all the users act in the same phase of the game: in this way, all actions performed by a user during step t are visible to other users only from step $t + 1$. The change of step is decided by the teacher, who rules and manages the game session. In this way the users, in our mind the kids with no or little knowledge on social media,

8. The word "bridge" here is not used with the usual meaning of the same word in graph theory, even though it is somehow related to it.

can easily focus on only one aspect of social networks at each step. The key intuition behind our serious game is that from step 4 the participants starts to become aware of the information diffusion processes. In fact, while during step 4 they can only see posts published by their friends, during step 5 (and the following steps) they may also see items posted by friends of friends: at this point, information can be propagated from a group to another one through the spurious links existing between them, thanks to the so-called *bridge users* defined beforehand, that for this reason play a key role in this game.

3.1.1 Preliminary steps and social graph generation

At the beginning of the game, a code is requested to users for joining the game session. Such code is unique, and it is automatically generated by the system when the teacher starts the game session. This solution permits to make user accounts ephemeral, thus avoiding the necessity of storing and managing persistent users' accounts and preventing any profiling activities. Once joined the game, each user is requested to type her name and to choose a profile picture from a set of predefined avatars provided by the game. It is worth noting that there is no need to enter the correct first and last names, but whenever real personal data are entered, they are available only to the teacher who started the related game session.

Each time a user joins the game, it is assigned in turn to one of the groups. The total number K of groups depends on the number N of users and is such that each group contains at least two users, and there are at least three groups: as a consequence, the minimal number of participants must be six. The number of groups is designed for fitting the number of students of a typical class in the Italian education system, composed by around 19 students in primary school and 21 students in lower secondary school[9]: with such numbers of participants, each group may contain from 3 to 4 users. The social graph is generated as follows. Users are first sorted according to their "arrival" time in the game. This choice ensure an intrinsic randomness in the generation of the social graph. Then, users are assigned to a group according to their order: the first user is assigned to the first group, the second user is assigned to the second group, the K-th user is assigned to the K-th group, the $(K+1)$-th user is assigned to the first group and so on. After that, an edge is added for each pair of users within the same group (thus, users within the same group are all connected to each other). Finally a ring is created by connecting each user to the following one, according to their order (the last user is connected with the first one). This guarantees that the network is connected, letting all users have potentially access to information posted by any other user after a reasonable number of iterations of the reactive phase explained later. Notice that our goal is not to generate scale-free or small-world networks [34], since there would be some users with few friends and other with many friends.

The total number of edges in the graph depends on N (the number of users) and K (the number of groups) and the formula used to calculate it ensures that, in a class with 20 students (and $K = 6$ groups), each user will be connected with other 4 or 5 friends. Moreover, the game experience would be the same independently if the game is played in very small classes (6-12 students) or in very large ones (25-35 students). Each user can check her friends' list by clicking on the corresponding button (see Fig. 3(b) that shows the game interface).

9. Data provided by ISTAT, the Italian National Institute of Statistics, available at http://www.istat.it/it/archivio/194422.

1. the users join the game session and configure their profile;
2. the users are randomly divided into groups and inserted into a social graph;
3. the users select the items to be posted (*active phase*);
4. the users like and/or share friends' posts (*first reactive phase*);
5. the users like and/or share posts liked or shared by friends (*second reactive phase*);
6. step 5 can be reiterated multiple times;
7. the users are notified with their behavioral scores.

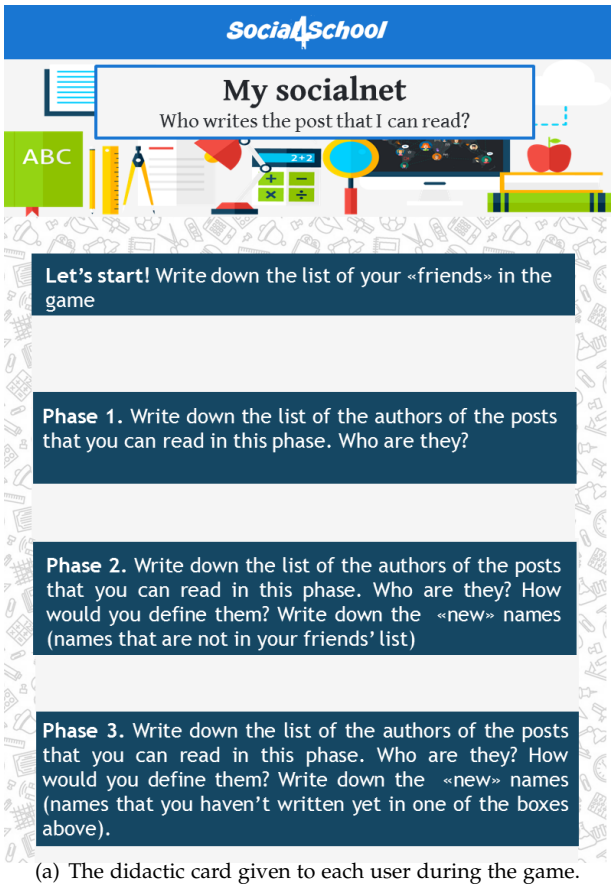
Fig. 2. The main steps defining the dynamics of the game.

3.1.2 Phases of the game

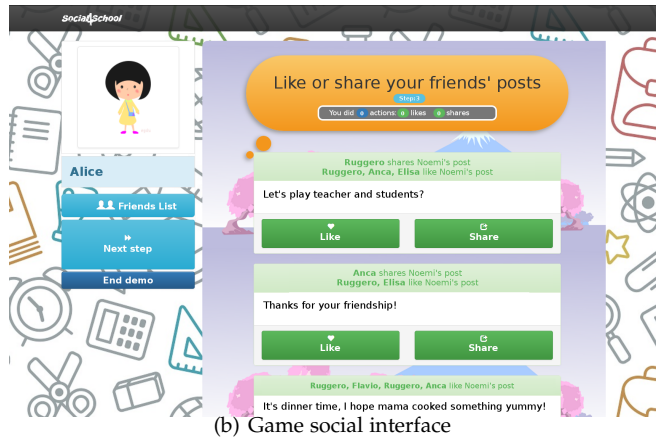
During the first phase of the game (called *active phase*) each user $u_i \in c_k$ may publish on her profile a post selected from the set of predefined posts P^k assigned to the group c_k. Note that users may not write posts on their own, because each post is assigned a predefined sensitivity score: it would be almost impossible to automatically compute it for user-generated content; moreover, in this way, we easily prevent users to write inappropriate content or a text which diverges from the objectives of the game. Users may undo and redo any posting action, but each item can be posted only once, and the minimum and maximum number of posts published on the profile are fixed by the teacher at the beginning of the game. In this phase users are asked to check their friends' list and to write the names on a didactic form (see Fig. 3(a)).

During the second phase (called *first reactive phase*), the game shows to each user the items posted by her friends in the previous phase. Users are allowed to perform two social actions on those posts: they can *like* or *share* them, and this information will be spread to their friends in the next step of the game. Again, users can undo and redo any social action, and the minimum and maximum number of social actions for each user is fixed by the teacher. It is worth noting that, in this phase, only bridge users can see the items posted by the users who do not belong to their group. Nevertheless, every user can read all the contents posted by their friends in the game. Children are asked to think about the authors of the posts they can read: in this way they can realize that this list coincides with their friends' list (see question 2 on the didactic card in Fig. 3(a).)

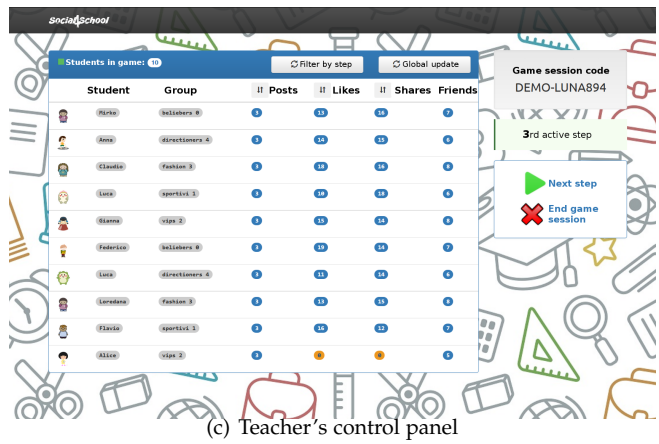
The third phase (called *second reactive phase*) is probably the most crucial of the game. In fact, in this phase the game shows to each user the items liked and shared by her friends, including the ones published by users that are not connected to her by direct friendship links. In this way the users start to discover and understand the dynamics of post propagation in social networks. Once again, children are asked to think



(a) The didactic card given to each user during the game.



(b) Game social interface



(c) Teacher's control panel

Fig. 3. The didactic card given to each user during the game (left) and two screenshots of the web application: the interface of the game as viewed by the participants (right, top) and the game control panel as viewed by the teacher (right, bottom).

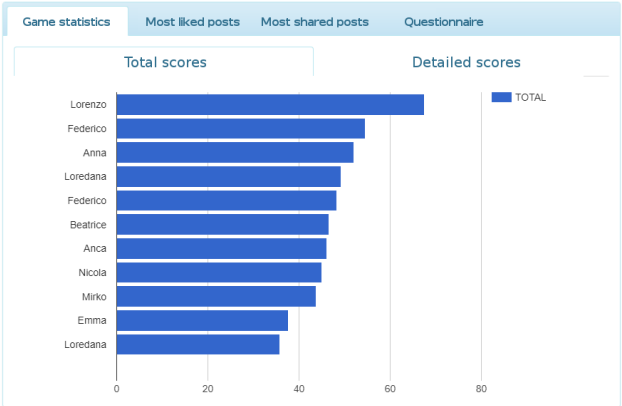
about their relationship with the authors of the posts they can read. The aim is to make them realize that in this phase thay can read *friends of friends'* posts. As in the previous phase, users can like or share the posts that appear in their feed. This phase can be iterated multiple times: at each iteration, a user may discover posts originally published by other users belonging to groups more and more distant to her group. Throught the different phases they are lead to figure out the diffusion of posts throught a social network that becomes wider and wider (friends $\rightarrow$ friends of friends $\rightarrow$ friends of friends of friends $\rightarrow$ ...). Fig. 3(b) shows the game interface during the reactive phases.

Our game is designed so that, in a typical class with 18 to 25 students (and $k = 6$) the average number of reactive phases required to make posts from all users potentially visible to everyone in the game is 4. This ensure that, with a limited number of phases, the students are able to observe and — in most cases — discover an information diffusion phenomenon. An example of node visibility according to the number of reactive phase is given in Fig. 1(b). During the first reactive phase, node 1 in the network of Fig. 1(a) (labeled with "0") is able to see all posts published by its direct friends (nodes labeled with "1"). During the second reactive phase, node 1 is able to see those posts of the friends of its friends (nodes labeled with "2") liked and shared by its friends. Finally, during the third reactive phase, node 1 may see the posts of node 7, provided that node 1's friends have liked or shared some of node 7's posts. Symmetrically, node 7 will be able to see posts of node 1 only during the third reactive phase.

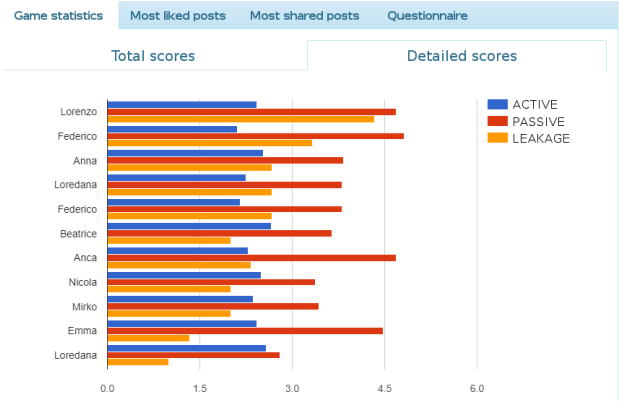
3.2 Score Computation

When the teacher decides to end the game session, all users are provided with a synthetic report describing how respectful they have been of their own and other users' privacy during the game. Such report is created using three scores we have identified for capturing different aspects of privacy in social media. The *Active Score* ($AS(u_i)$) can be defined as the personal impact of user u_i on other users' privacy, and it is calculated as 5 (the maximal score of an item) minus the average score of the social actions performed by u_i, while the *Passive Score* ($PS(u_i)$) is defined as the personal impact of user u_i on her own privacy, and it is calculated as 5 minus the average score of the items published by u_i in the active phase.

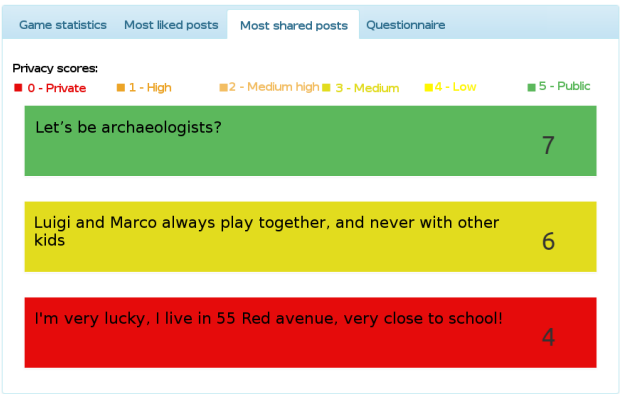
The Active and Passive scores capture the impact of each user on her own and other users' privacy and depends uniquely on her own behavior. The last score, instead, is a systemic score that measures to what extent the privacy of user u_i has been compromised by the actions of other users. It is called *Leakage Score* ($LS(u_i)$), and it can be defined as the overall privacy leakage of user u_i. This score depends on how many times sensitive posts of user u_i have been liked



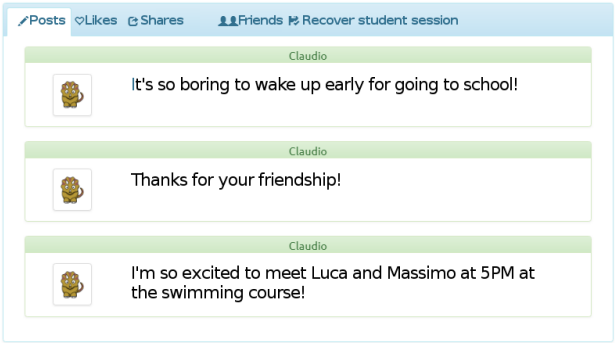
(a) Total score.



(b) Detailed scores.



(c) Most shared posts.



(d) Post and actions of a single student.

Fig. 4. Interactive report generated at the end of any game session. Information provided by the different sections of the report can help teachers conduct their classroom activities.

or shared by other users, and is calculated considering that actions performed during the last phases of the game have a larger negative impact on the score than the ones performed in the first phases. In fact, if information has survived until the very last steps, it can potentially still spread across a larger part of the network.

All the three scores range between 0 (worst case) and 5 (best case). Note that actions "like" and "share" have the same impact on the calculation of all scores, because the result of these actions is the same: to show a content to all the friends of a user. Scores are explicitly provided to user for provoking curiosity and raising discussions among the participants, and the game offers a special notification to the three users who perform the best according to the sum of active and passive score for offering a form of competition between participants.

3.3 Teacher's Panel

As already pointed out, all game steps are driven and controlled by a person (a sort of "master") that, in schools, is identified with the teacher. Teachers have a personal profile page on *Social4School*, accessed through login and password, where they have the possibility to start a new session, through a game control panel, or to visualize the statistical report generated at the end of any of their previous game sessions, through a game statistics panel. The *game control panel* (Fig. 3(c)) allows the teacher to configure, start, manage and terminate the game sessions. The *game statistics panel* (see Fig. 4) provides both a synthetic view (average scores of the game) and detailed view on all participants' actions and scores. All this information is intended as a support for any educational activity envisaging discussions around the game sessions, in an interactive and participatory way.

3.4 Design methodology and implementation

The educative platform implementing our game, named *Social4School*[10], has been realized as a responsive web application written in HTML5, CSS3, PHP and Javascript, and runs under the Apache Web Server. Data are stored in a relational database managed with MariaDB. *Social4School* currently runs on a non-dedicated dual-processor Intel Xeon 5140 server equipped with 4GB RAM, having Linux (Kernel release 4.6.4) as operating system. The server is physically hosted at the Department of Computer Science of the University of Turin. Since the initial target users are Italian primary and lower secondary school students, the website and the game are in Italian. The web application also features a "demo" mode that can be used to test the game experience at any time.

Game scenarios are handled as plugins to enable the customization of the game session. Each scenario consists in a background image and a set of predefined groups

10. Available online at http://www.social4school.eu

with their avatars (for the participant profile pictures) and their set of posts with the corresponding sensitivity scores. It is worth noting that there is no need to modify the source code of the application for adding new scenarios. For each group c_k, each post p_m^k as been assigned a score $score(p_m^k) \in \{0, 1, \ldots, 5\}$ equal to mean of the scores given by four different annotators. Hence, the score of each post does not simply reflects the sensibility of one single person.

The realization of the web application has been conducted following a participatory design process involving three computer scientists, a UI/UX expert, two Bachelor's students and a primary school teacher. In a first phase (winter 2015/2016), a fully-functional prototype has been designed and implemented following the Agile approach. It has been tested by the primary school teacher, who participated in the successive development phase and provided both the sentences to be posted and suggestions on the teacher's panel interface. Then, four test sessions were organized with two teachers and four primary school classes. During these test session, we monitored the reactions of the students, noted all major and minor bugs, collected the suggestions of the teachers and edited a final report with all necessary changes and improvements. With the help of the UI/UX expert, we released a new improved build of the web application and we finally tested it with the same classes and teachers. After the correction of some minor bugs, we finally released the application in fall 2016. Hence, the overall development stage lasted approximately one year.

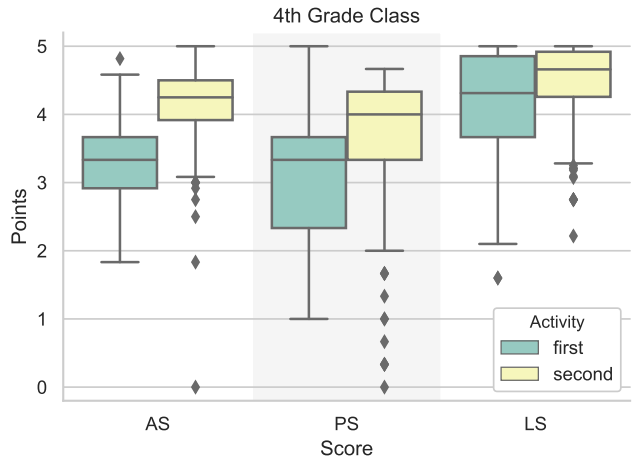
4 Experimental results

In this section we report the results of an extensive experiment we conducted in seven Italian primary school complexes. The goals of our experimentation were: i) to evaluate the effectiveness of an educational activity supported by our tool to increase the awareness of children about privacy in social media w.r.t. the specific situations addressed in our application (i.e., the increased ability to recognize risky scenarios that are similar to those presented in Social4School); ii) to measure the effectiveness of the educational activities supported by Social4School in augmenting the awareness about privacy in more general situations not specifically addressed by our application (i.e., the increased ability to recognize risky behaviors that are different from those simulated in the web application); iii) to obtain a general assessment of our approach and web platform, together with some suggestions from the teachers involved in our activities.

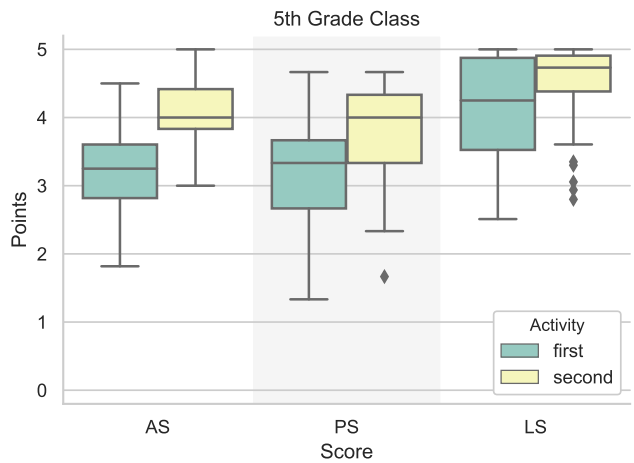
Before entering the details of the results, in the following we present the experimental settings by describing the implementation of our application, how we recruited the participants and the methodology of our experimentation.

4.1 Recruitment

With the double goal of testing our web application and performing a preliminary assessment of its validity and utility, between March 2016 and May 2016, we set up an experiment in an Italian primary school, in the Turin area. The results were presented on December 2016, during an event named



(a) Game scores (4th-grade students)



(b) Passive score (5th-grade students)

Fig. 5. Active, Passive and Leakage scores distributions among 4th-grade students (a) and 5th-grade students (b) at the end of each game session.

Teachers for Teachers (T4T)[11] at the Department of Computer Science of the University of Turin. During this event, we launched our recruitment campaign aimed at finding some voluntary primary schools interested in participating in our experiment. In the following weeks, four institutions from different parts of the Piedmont region expressed their interest in our experiment. Thus, we established a formal agreement with all those schools, set up a privacy policy with the help of the Law Office of the University of Turin, distributed the informed consent to the parents of all children possibly involved in our experiment and ask them for the signed privacy consent form. Only those children whose parents had signed the privacy consent form were allowed to participate in our experiment. A reference person, in charge of other teachers' training activities and organization of the experience, was chosen by each school. Overall, 22 classes were involved in our study, 14 fourth-grade classes (kids aged 9 to 10 years) and 8 fifth-grade classes (kids aged 10 to 11 years). Overall, around 450 children and 22 teachers are involved in our study.

11. http://t4t.di.unito.it/

TABLE 1
Survey questions and possible answers. In questions Q1 and Q3 multiple choices are allowed. A sensitivity value is associated to each answer. Within the same question, sensitivity values sum up to 1.

Quest. No.	Question text	Answ. No.	Possible answer text	Sensitivity
Q1	Imagine being enrolled in a social network, what would you use it for?	1.1	Chatting with my friends	0.00
		1.2	Posting my thouthts	0.10
		1.3	Commenting my friends' posts	0.10
		1.4	Writing in chat groups	0.10
		1.5	Talking about what happens to me	0.20
		1.6	Posting my personal photos	0.25
		1.7	Posting photos in chat groups	0.25
Q2	Are you willing to publish the photo you just took on a vacation with your parents?	2.1	No	0.00
		2.2	Yes	1.00
Q3	Your friend has just posted a photo taken on vacation and you enjoy it so much. What would you do?	3.1	I'd tell her/him privately how much I like it	0.00
		3.2	I'd push the like button	0.2
		3.3	I'd put a comment on it	0.3
		3.4	I'd share it	0.50

4.2 Methodology

Phase 1 The experiment was conducted as follows. First, all classes were randomly divided into two groups: *control* classes and *experimental* classes. In February and March 2017, the participants played a game session under the control of their teacher (supported by us) without being aware of the real goal of the activity: they have only been informed that they were going to play a game on computer. The session consisted of an active phase followed by one first reactive phase and two second reactive phases. At the end of the game the students received a ranking and some recommendations that have been discussed later in the classroom within a participatory education activity held by their teacher. Before leaving the game, children in *control* classes only were asked to answer a small questionnaire consisting in the three simple questions shown in Table 1. Notice that our application focus on written posts, while some questions of the survey are also related to pictures. Moreover, all question are related to more general privacy issues in online social network (such as, putting friends' privacy at risk or using social media for more or less risky activities).

Phase 2 Few days after the game session, the teacher gave a lesson to their students on the topic of privacy on the Internet, with a particular focus on social networks. We did not participate to such lesson, neither we gave special suggestions or materials: each teacher prepared the lesson on his own, employing our system and the results of game session as her wish.

At the end of the experiment we interviewed the teachers to understand how they had used the report during this phase. Despite some differences on the amount of time they spent on the activity, they all basically used the report on the game session to discuss the following points with the students:

- most liked/shared post and their "colours" (Fig. 4(c)): the aim was to make students think about what they had liked/shared;
- post propagation (using the didactic card in Fig. 3(a)): students were encouraged to think about the consequences of their actions in the game and to figure out the path of a post in the social network. Some teachers used the report to recreate and display (on a blackboard or screen) the route taken by one or more posts in the game;
- each action on a post in the online social network has a "weight" and this weight depends on the content of the post. While meditating on these points, students start to understand the criteria used by the game to classify them (see Fig. 4(a));
- each action on a post can impact on one's own privacy and other users' privacy. This point has been discussed using detailed scores (see section 3.2 and Fig. 4(b)).

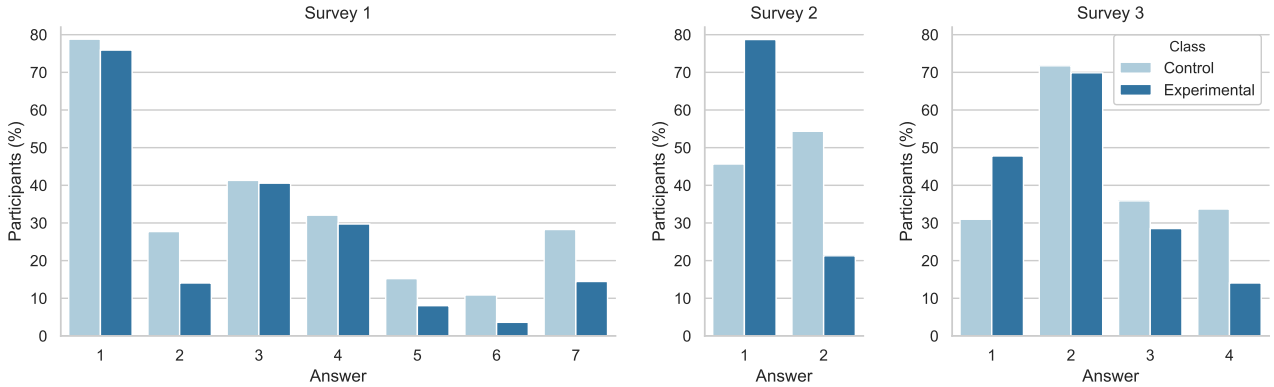
At the end of the general discussion, the teachers spent some more one by one time with students to analyze their actions in the game.

Phase 3

After a couple of months, in May and June 2017 the same students played another game session under the direction of the same teacher. At the end of this activity, children in the *experimental* classes only answered the same questionnaire as their pairs. In summary, the difference between control classes and experimental classes was the time they where proposed the questionnaire. Control classes answered before their activity in Social4School was analyzed, while experimental one have attended the whole activity before answering the questionnaire.

4.3 Results: privacy scores

As first analysis, we measure and compare the average Active Score (AS), Passive Score (PS) and Leakage Score (LS) for all participants within the two game sessions. Notice that it is not possible to compare the scores for each individual child, since participation was maintained anonymous and it is impossible to match the scores of the same student computed at the end of the two activities. This is mainly due to the following privacy policy requirements imposed by the Italian Law, which is particularly stringent on studies involving minors: i) individual profiling should



(a) Question Q1 (b) Question Q2 (c) Question Q3

Fig. 6. Survey results: the height of each bar indicates the percentage of students that have chosen the correspondent answer within each group. See Table 1 for retrieving each question and answer text.

be prevented and ii) the anonymity of the young respondent should be preserved as much as possible. However, this is not a problem, since we are interested in the average behavior and to the overall distribution of the three scores computed at the end of the two activities.

To compare the global effects of our activity, we compare the distributions of the three scores on the whole population. The observed scores are plotted in Fig. 5. In particular, Fig. 5(a) shows the three score distributions computed at the end of the first and second activities in the 4th-grade classes, while Fig. 5(b) illustrates the distribution of the scores in the 5th-grade classes at the end of the two game sessions. It can be observed that, in the second game session, the distribution of all scores are shifted to higher (and safer) values. To assess the statistical significance of this improvement, we perform an unpaired two-tailed t-test for unequal sample sizes. This choice is due to the fact that the two samples are not exactly the same, for two reasons: first, it is not possible to match two scores obtained at the end of the two activities by the same students; second, the two samples are not equal in size, since some students were missing in one of the two sessions. We used the Benjamini-Hochberg correction procedure to controls the false discovery rate [35]. The results of this test clearly indicate ($p < 0.0005$) that the null hypothesis that the two sets of scores are drawn from the same distribution can be comfortably rejected: the improvements are statistically significant.

We also verify whether the improvement are independent from the grade of the students. To do that, we perform two unpaired t-tests for each score: in the first test, we compare the results achieved at the end of the first game session by the 4th and 5th grade students; in the second test we perform the same comparison at the end of the second game session. In this case, the null hypothesis cannot be rejected ($p > 0.1$ for all scores), i.e., the results are not significantly dependent on the age of the participants.

4.4 Survey results

The second experimental result concerns the analysis of the survey submitted to the students at the end of the first game session (control classes) or at the end of the second game session (experimental classes). To perform this analysis, we first compare the overall results of the two groups. According to Fig. 6, the students in experimental classes assume a safer behavior towards privacy than their control pairs.

In details, in the first question (Fig. 6(a)) the students belonging to the experimental classes show a more careful intention towards social media usages: chatting is by far the preferred option in both groups, but the experimental group loses interests in other — intrinsically less secure — activities, such as posting personal thoughts, facts and pictures. Interestingly, although group chats have not been the focus of our educational activities, the experimental group seems to perceive the dangers of posting personal pictures in group chats.

The answers to the second question (Fig. 6(b)) show that the students who completed the whole activity (experimental classes) would undertake a more careful behavior w.r.t. their own and their family's privacy. The polarity of the answers changes drastically, with a majority of students in the experimental group (79%) preferring not to share family vacation pictures, compared to the inverted proportion observed in the control group (54% of the students in this group are willing to share pictures just taken during a vacation with the family). Similarly, the answers to question Q3 (see Fig. 6(c)) show that the experimental group would have a greater attention to their friends' privacy, by preferring more safe reactions (private messages, likes) to more harmful ones (comments, shares).

To assess the statistical validity of this survey, we perform the following analysis. We assign a sensitivity weight between 0 and 1 to each possible answer of every question. The meaning of the sensitivity weight is as follows: the higher the weight, the most harmful the answer w.r.t. privacy. Weights are such that within each question they sum up to one. We then measure a *sensitivity score* for each question and each participant. According to this schema, for any given question, a participant obtains a score equal to one if she chooses all harmful options; she obtains a zero-score if no harmful answer is chosen. The sensitivity weights assigned to each answer are given in Table 1 (last column) while the results of this analysis are given in Table 2.

TABLE 2
Average sensitivity scores and t-test results per class group and class grade. Overall results are also reported. The Benjamini-Hochberg correction procedure has been used to controls the false discovery rate [35].

Qst.	4th-grade students			5th-grade students			All students		
	control	experimental	p-value	control	experimental	p-value	control	experimental	p-value
Q1	0.238($\pm$0.208)	0.156($\pm$0.148)	< 0.005	0.216($\pm$0.230)	0.120($\pm$0.139)	< 0.005	0.229($\pm$0.218)	0.146($\pm$0.146)	< 0.005
Q2	0.555($\pm$0.497)	0.227($\pm$0.419)	< 0.005	0.527($\pm$0.499)	0.178($\pm$0.383)	< 0.005	0.543($\pm$0.498)	0.213($\pm$0.409)	< 0.005
Q3	0.455($\pm$0.304)	0.301($\pm$0.276)	< 0.005	**0.368($\pm$0.294)**	**0.284($\pm$0.256)**	> 0.1	0.420($\pm$0.303)	0.296($\pm$0.270)	< 0.005
All	1.247($\pm$0.770)	0.684($\pm$0.634)	< 0.005	1.111($\pm$0.818)	0.582($\pm$0.573)	< 0.005	1.192($\pm$0.793)	0.654 ($\pm$0.619)	< 0.005

In general we observe that all average sensitivity scores (including their sum) are lower in the experimental classes than in the control ones, thus confirming the outcomes of the previous analysis. Furthermore, the differences are statistically significant (p-values of the unpaired two-tailed t-test are < 0.005) with the only exception of question Q3 in the 5th-grade classes (highlighted in bold). However, the differences in overall scores (last row in Table 2) are always statistically significant ($p < 0.005$). Finally, it is worth noting that, even in this case, there are no statistically significant differences between the two class grades (p-value> 0.05): the educational activities had the same impact on privacy awareness regardless of the participants' age.

4.5 Teachers survey

In this section we present the results of a survey that we submitted to the teachers who conducted the activities at the end of the experience with Social4School. We also report the main outcomes of one-on-one interviews to obtain feedbacks from all participants. Among the main objectives of the survey there were: i) extraction of best practices to maximize Social4school effectiveness as a class activity; ii) comprehension of the interplay between the Social4School game, teacher activity in the class and, as a consequence, teachers' training needs. In the following, we first describe the survey design and methodology; then, we report the results and a summary of the interviews.

4.5.1 Survey methods and design

The survey was designed to help us understand different subjective aspects of the activity as follows:

1) perception about the effectiveness in terms of acquired skills/knowledge on both students and teachers side;
2) evaluation of the Social4School experience on both teachers and students' perspective;
3) needs for complementary training on privacy awareness on social networks to complete the activity with Social4School.

We chose a survey conducted through an online questionnaire in order to make it as convenient as possible particularly given that our main target, teachers, are usually very busy and work in many different schools. Participants were offered no reward except a copy of the research results, when available. We specifically targeted teachers involved in schools experimentation. In the fist part of the survey we collected participants' age and years of teaching experience to be able to evaluate the potential impact on the above objectives. The remaining part of the questionnaire was made up of three main parts related to the above evaluation objectives.

Perception about the effectiveness in terms of acquired skills/knowledge. In order to assess Social4School effectiveness we dedicated the first part of the survey to ask teachers whether they had found Social4School effective with respect to three distinct measures (*understanding*, *interest* and *awareness*) concerning three issues: *spread of information in the internet*, *privacy in online social networks* and *the related protection mechanisms*. Our purpose was to investigate the interplay among understanding, interest and awareness after Social4School experience since many surveys ([1], [2], [3], [4]) show that both adults and minors are neither aware of nor interested in the consequences of privacy leakage in the internet.

Evaluation of Social4School experience on both teachers and students' perspective. We asked teachers to evaluate children's interest and motivation in Social4School activity. We also considered the following factors (see questions in Tables 3 and 4):

- teachers' involvement in the activity (their role and the number of hours spent on phase 2);
- teachers' motivation and attitude;
- support from parents and from school management.

Our aim was to collect evidences about the overall experience of the teachers, in order to assess both the satisfaction level and the working background (potential obstacles, support from parents/principals).

Complementary training on privacy awareness in social networks to complete the activity with Social4School. During the second game session (after the classroom activity described in Phase 2, Section 4.2) many teachers expressed the need for training and guidance on online privacy related issues. We included both questions on past activities attended by teachers (in order to assess the impact on the Social4school experience) and on future needs on training to collect feedbacks and suggestion for our ongoing work regarding the production of didactic sources on the subject.

4.5.2 Survey results

The results have been classified based on themes developed from the research questions.

Participants profile. 15 teachers from the schools cited in Section 4.1 fully answered the survey. Among them, one is male. Participants age ranges from 30-40 (13%), 40-50 (53%) to 50-60 (34%). Most of the teachers have more than 10 years

TABLE 3
Results of questions about teachers involvement in Social4School and their evaluation about students attitude during the activity.

Quest. No.	Question text	Possible answer text	M
Q 25	Involvement in Social4School	my class(es) was involved in Social4School	33%
		my class(es) was involved in Social4School and I held the participatory education activity between the two game sessions	67%
Q 26	How many hours did you spend discussing about privacy related issue between the two activities with Social4School?	2-3	58%
		8-12	33 %
		25	9%
Q 27	Using Social4School did you notice gender differences regarding attitudes about social networks' protection of privacy and information?	Yes	60%
		No	33%
		I don't know	7%
Q 28	Students' motivation in Social4School activity	Low	0%
		Moderate	27%
		High	63%
Q 29	How would you assess the students' interest in (Social4School activity+related issues)?	Absent	0%
		Limited	0%
		Quite limited	0%
		Great	20%
		Very great	80%

in teaching experience (87%) while the remaining 13% have from 3 to 10 years of experience. We did not find any impact of age and past teaching experience on the answers to the remaining questions (discussed in the following).

Teachers' perspective about their acquired understanding, interest and awareness about the three issues (spread of information in the internet, privacy in online social networks). These questions had to be answered using a six-point Likert-scale, with responses ranked from 1 (strongly disagree) to 6 (strongly agree). The responses of each question were averaged, and the standard deviation was obtained (we omit the table for brevity). Almost all mean scores are higher than or equal to 5 indicating a positive impact on both students and teachers' perception about online privacy related issues. Mean scores lower than 5 are related to students understanding, interest and awareness about protection mechanisms in online social networks. The reason is that Social4School simulation does not specifically focus on protection mechanisms which will be subject of a future extension. Other mean scores lower than 5 are those related to students' *awareness* about the three issues. This aspect was investigated during the interviews: some teacher claimed that, despite the utility of Social4School, a complete awareness can only be reached through real experiences. It is interesting to note that most of the teachers that expressed a lower agreement grade on questions related to awareness, were those that had previously attended courses on the subject (see questions in Table 4). This can be explained by the fact that previous activities had raised respondents awareness.

Teachers' involvement in Social4School and their evaluation about students attitude during the activity (see Table 3, questions 25-29). Among the involved teachers, 67% also held the participatory education activity between the two game sessions spending a variable number of hours on it. During Social4School activities 60% noticed gender differences between students. This result suggests further investigations on gender differences w.r.t. Social4school use and impact. Results about questions 28-29 confirmed our intuition about students interest and motivation towards Social4School (students motivation was high according to 63% of teachers while interest was very great according to 80%).

Teachers' attitude and related background (Table 4, questions 30-33). The answers confirm teachers' interests in online privacy related issues. Teachers also evaluated positively parents' attitude (80% found it quite positive). It is interesting to remark that 1 out of 3 teachers is unaware about school management attitude confirming the high level of personal motivation in joining Social4School despite the working context. We investigated this aspect in the interviews that followed the survey analysis: the teachers explained that, despite the interest from the school managers, they would expect more initiative from their institutions. Although they did not experienced any obstacles, they would like to receive more help in the organization of the activities and related training.

Teachers past experience and future needs on training activities dedicated to online privacy related issues (Table 5, questions 34-39). The outcomes highlight the lack of training and material on social media and privacy related problems. Despite the strong motivation about the topic, only 1 out of 3 teachers evaluates her past training and related aiding materials as sufficient. Indeed, 100% claim they need more knowledge about social media education.

4.5.3 Interviews

To further investigate some critical aspects emerged from the survey, the participating teachers were interviewed to provide opinions and suggestions. We collected many comments from participants encompassing the overall satisfaction, as well as suggestion to improve and extend So-

TABLE 4
Results related to questions on teachers attitude and related background.

Quest. No.	Question text	Possible answer text	M
Q 30	What are the reasons to teach about privacy related issues	I think it is important	100%
		It is in the curricula	0%
		The school management requires it	0%
Q 31	Do you think it is important to teach about privacy related issues at primary school?	Completely unimportant	0%
		Quite unimportant	0%
		Quite important	13%
		Very important	87%
Q 32	How do you assess the interest shown by the school management?	They are uninterested	0%
		They are quite interested	27%
		They are very interested	40%
		I don't know	33%
Q 33	How do you assess parents' attitude towards Social4School activity?	Very negative	0%
		Quite negative	0%
		Indifferent	7%
		Quite positive	80%
		Very positive	0%
		Not known	13%

TABLE 5
Results related to questions about teachers needs and experience on training activities on online privacy related issues.

Quest. No.	Question text	Possible answer text	M
Q 34	Have you participated to other training activities about social media education related issues?	Never	74%
		Once	13%
		More then once	13%
Q 35	How would you assess the availability of of teaching aids relating to social media education related issues?	Sufficient	33%
		Quite limited	47%
		Non existent	20%
Q 36	To what extent has social media education related issues dealt with in the context of your teacher training?	Sufficient	33%
		Limited	47%
		Non existent	20%
Q 37	Guidelines for teaching social media education related issues should be	More	93%
		Less	7%
		Are adequate	0%
Q 38	Do you need more knowledge about social media education related issues?	Yes	100%
		No	0%
Q 39	What kind of training would you like as an integration of Social4School activity?	Publications (papers, books)	6%
		Teachers training courses	59%
		Online courses/material	35%

cial4School. Answers related to the activity held in phase 2 have already been summarized and reported in Section 4.2.

Overall satisfaction. The participating teachers were really satisfied and confirmed the initial strong motivation in the activity despite some difficulties. Some the comments are as follows:

"Despite it was difficult to add an extra activity (activities are planned the year before) I was enthusiastic about Social4School."

"We really think online privacy issues are of primary importance and this kind of activities should be promoted by school managers."

"We would like to adopt Social4School as a permanent activity proposed to all classes every year."

"The use of activities like Social4School can be very effective especially in geographic areas with social problems and differences."

Students experience and attitude. In the interviews teachers shared their experience during the participatory activities between the two game sessions. They were positively impressed by the way children lead the discussion and by the high cooperation spirit they showed. Here some excerpt from the interviews:

"I would have expected they were more passive, instead they drove almost all the discussion."

"They spent lot of time explaining each other their point of view on privacy online issues involved in the game and in giving advices on how to improve Social4school score in the second activity."

Future extensions. The interaction with teachers gave us many important feedbacks to plan future works and extensions. The first suggestion we got is about parents training on online privacy issues. Teachers reported that, despite parents willingness towards Social4School, most of the time they are almost completely unaware of the importance of online privacy. The second suggestion was about training materials for teachers as a complementary aid in holding Social4School sessions and consequent participatory activities. They feel the need for dedicated training to face students who are immersed in the word of online social networks.

5 Conclusions

With the final goal of enhancing user perception and awareness of privacy, we have designed and implemented a serious game that can be adopted as educational support to activities involving digital literacy issues in primary and lower secondary schools. The game has been tested in seven Italian primary schools complexes with success. The results have shown the effectiveness of our interactive gamification approach in stimulating the curiosity of the students that show an improved awareness on the spread of private information in online social networks.

As ongoing work, we are developing two native mobile applications (a student application and a teacher one) intended for those schools who already own tablets or other mobile devices. The first release is already available on the Google Play Store[12]. Some further improvements will include the possibility of adding more complex scenarios for high school students and adults as well as the development of a collaborative workspace for the creation of new scenarios and contents.

Moreover, since the specific training of educational staff is extremely important for the correct use of our application, we will design and implement a set of comprehensive didactic activities together with the related teaching materials and resources. We plan to share all so-produced materials with the teaching staff of the Italian primary and lower secondary schools and to cooperate with other countries to provide localized versions of Social4School together with the associated didactic resources.

Finally, thanks to a new collaborative research project with the Department of Philosophy and Educational Sciences and the Department of Psychology, we will conduct a new extensive experiment taking into account how teachers use our application, to see how this influences the learning results of school children, with the aim of proposing the most effective teaching methodology.

Acknowledgment

We wish to thank: the anonymous reviewers for their valuable comments; all the principals who helped us organize the experimental activities in their schools; the teachers who conducted the educational activities; Paolo Maino and Manuel Marino who developed the Android applications; Maurizia Gai, Rosa Pagella, Bruna Pezzana and Barbara Demo for stimulating discussions; Mario Alovisio who assessed the privacy policy of our application and experiment; last, but not least, Gianpiero Di Blasi who participated to the initial phase of the project. This work is co-funded by Fondazione CRT (grant numbers 2015-1638 and 2017-2323).

12. https://play.google.com/store/apps/developer?id=Ruggero+G.+Pensa

References

[1] Y. Liu, P. K. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: user expectations vs. reality," in *Proceedings of ACM SIGCOMM IMC '11*. ACM, 2011, pp. 61–70.

[2] M. Kosinski, D. Stillwell, and T. Graepel, "Private traits and attributes are predictable from digital records of human behavior," *PNAS*, vol. 110, no. 15, pp. 5802–5805, 2013.

[3] M. Furini and V. Tamanini, "Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions," *Multimedia Tools Appl.*, vol. 74, no. 21, pp. 9795–9825, 2015.

[4] Ipsos Public Affairs, "Safer internet day study 2015: i nativi digitali conoscono veramente il loro ambiente?" IPSOS, Tech. Rep., 2015. [Online]. Available: https://www.savethechildren.it/sites/default/files/files/uploads/pubblicazioni/safer-internet-day-study-2015-i-nativi-digitali-conoscono-veramente-il-loro-ambiente_0.pdf

[5] P. Dillenbourg, *Collaborative Learning: Cognitive and Computational Approaches (Advances in Learning and Instruction)*, 2nd ed. Oxford, UK: Pergamon Press, 1999.

[6] C. C. Bonwell and J. A. Eison, *Active learning : creating excitement in the classroom*. Washington, DC, USA: ERIC Clearinghouse on Higher Education, George Washington University, 1991.

[7] G. Trentin, *Networked Collaborative Learning*. Cambridge, UK: Chandos Publishing, 2010.

[8] A. Mislove, B. Viswanath, P. K. Gummadi, and P. Druschel, "You are who you know: inferring user profiles in online social networks," in *Proceedings of WSDM 2010*. ACM, 2010, pp. 251–260.

[9] L. Zou, L. Chen, and M. T. Özsu, "K-automorphism: A general framework for privacy preserving network publication," *PVLDB*, vol. 2, no. 1, pp. 946–957, 2009.

[10] K. Liu and E. Terzi, "Towards identity anonymization on graphs," in *Proceedings of ACM SIGMOD 2008*. ACM, 2008, pp. 93–106.

[11] B. Zhou and J. Pei, "The *k*-anonymity and *l*-diversity approaches for privacy preservation in social networks against neighborhood attacks," *Knowl. Inf. Syst.*, vol. 28, no. 1, pp. 47–77, 2011.

[12] X. Ying and X. Wu, "On link privacy in randomizing social networks," *Knowl. Inf. Syst.*, vol. 28, no. 3, pp. 645–663, 2011.

[13] N. Vuokko and E. Terzi, "Reconstructing randomized social networks," in *Proceedings of SIAM SDM 2010*. SIAM, 2010, pp. 49–59.

[14] M. Hay, G. Miklau, D. Jensen, D. F. Towsley, and P. Weis, "Resisting structural re-identification in anonymized social networks," *PVLDB*, vol. 1, no. 1, pp. 102–114, 2008.

[15] G. Cormode, D. Srivastava, S. Bhagat, and B. Krishnamurthy, "Class-based graph anonymization for social network data," *PVLDB*, vol. 2, no. 1, pp. 766–777, 2009.

[16] M. Hay, C. Li, G. Miklau, and D. Jensen, "Accurate estimation of the degree distribution of private networks," in *Proceedings of ICDM 2009*. IEEE, 2009, pp. 169–178.

[17] C. Task and C. Clifton, "A guide to differential privacy theory in social network analysis," in *Proceedings of the International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2012, Istanbul, Turkey, 26-29 August 2012*. IEEE Computer Society, 2012, pp. 411–417.

[18] J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social media," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 7, pp. 1851–1863, 2016.

[19] K. Liu and E. Terzi, "A framework for computing the privacy scores of users in online social networks," *TKDD*, vol. 5, no. 1, pp. 6:1–6:30, 2010.

[20] R. G. Pensa and G. D. Blasi, "A privacy self-assessment framework for online social networks," *Expert Systems with Applications*, vol. 86, pp. 18 – 31, 2017.

[21] A. Cetto, M. Netter, G. Pernul, C. Richthammer, M. Riesner, C. Roth, and J. Sänger, "Friend inspector: A serious game to enhance privacy awareness in social networks," in *Proceedings of IDGEI 2014*, 2014.

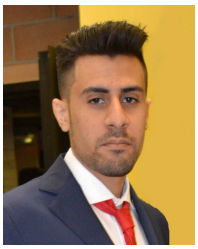
[22] E. Litt, "Understanding social network site users' privacy tool use," *Computers in Human Behavior*, vol. 29, no. 4, pp. 1649–1656, 2013.

[23] G. Misra and J. M. Such, "How socially aware are social media privacy controls?" *IEEE Computer*, vol. 49, no. 3, pp. 96–99, 2016.
[24] L. Bioglio and R. G. Pensa, "Impact of neighbors on the privacy of individuals in online social networks," in *Proceesings of the International Conference on Computational Science, ICCS 2017, 12-14 June 2017, Zurich, Switzerland*, ser. Procedia Computer Science, vol. 108. Elsevier, 2017, pp. 28–37.
[25] H. Choi, J. Park, and Y. Jung, "The role of privacy fatigue in online privacy behavior," *Computers in Human Behavior*, vol. 81, pp. 42–51, 2018.
[26] C. Aldrich, *Simulations and the Future of Learning: An Innovative (and Perhaps Revolutionary) Approach to e-Learning*. John Wiley., 2004.
[27] Y. B. Kafai, "Playing and making games for learning," *Games and Culture*, vol. 1, no. 1, pp. 36–40, 2006. [Online]. Available: http://dx.doi.org/10.1177/1555412005281767
[28] M. Prensky, "Digital game-based learning," *Comput. Entertain.*, vol. 1, no. 1, pp. 21–21, Oct. 2003. [Online]. Available: http://doi.acm.org/10.1145/950566.950596
[29] C. Hung, F. Kuo, J. C. Sun, and P. Yu, "An interactive game approachfor improving students' learning performance in multi-touchgame-based learning," *IEEE Trans. Learning Tech.*, vol. 7, no. 1, pp. 31–37, 2014.
[30] C.-H. Su and C.-H. Cheng, "A mobile gamification learning system for improving the learning motivation and achievements," *Journal of Computer Assisted Learning*, vol. 31, no. 3, pp. 268–286, 2015.
[31] A. Domínguez, J. Saenz-de-Navarrete, L. de Marcos, L. F. Sanz, C. Pagés, and J. Martínez, "Gamifying learning experiences: Practical implications and outcomes," *Computers & Education*, vol. 63, pp. 380–392, 2013.
[32] J. Torrente, B. Borro-Escribano, M. Freire, Á. del Blanco, E. J. Marchiori, I. Martínez-Ortiz, P. Moreno-Ger, and B. Fernández-Manjón, "Development of game-like simulations for procedural knowledge in healthcare education," *IEEE Trans. Learning Tech.*, vol. 7, no. 1, pp. 69–82, 2014.
[33] L. de Marcos, A. Domínguez, J. Saenz-de-Navarrete, and C. Pagés, "An empirical study comparing gamification and social networking on e-learning," *Computers & Education*, vol. 75, pp. 82–91, 2014.
[34] M. Newman, *Networks: An Introduction*. New York, NY, USA: Oxford University Press, Inc., 2010.
[35] Y. Benjamini and Y. Hochberg, "Controlling the false discovery rate: A practical and powerful approach to multiple testing," *Journal of the Royal Statistical Society Series B (Methodological)*, vol. 57, no. 1, pp. 289–300, 1995.

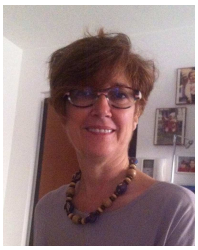
Livio Bioglio received his M.Sc. degree in Computer Science in 2009 at the University of Turin, and his Ph.D. in Computer Science in 2013, in the same institution. During his Ph.D. studies he focused on Type Theory and theoretical modeling of biological systems. In 2013 he was a Post-doc at INSERM, Paris (France), working on complex systems and epidemiology, in particular computational models for analyzing the spread of influenza in realistic populations. Since 2016 he is Post-doc at the University of Turin, studying the diffusion of information in social networks, with focus on privacy concerns.

Sara Capecchi received the M.Sc. degree in Computer Science at the University of Florence in 2002 and a Ph.D. in Computer Science (2003-2006) at the Department of Computer Science, University of Florence. From 2005 to 2007 she was research associate at the Department of Mathematics and Computer Science, University of Catania. From 2008 to 2010 she was post-doc research associate at Department of Computer Science, University of Turin. Since 2010, she is Assistant Professor at the Department of Computer Science, University of Turin. Her main research interests include conceptual models for trust and reputation systems and static analysis of distributed systems with a focus on information leakage and access control.

Federico Peiretti received the B.Sc. degree in Computer Science at the University of Turin in 2016. From 2016 to 2017 he was research fellow at the Department of Computer Science, University of Turin.



Dennis Sayed received the M.Sc. degree in Computer Science at the University of Turin in 2018. In 2016 he was research fellow at the Department of Computer Science, University of Turin.



Antonella Torasso received a degree in Orthopsychiatry at the Institute of Studi Superiori "Giuseppe Toniolo" of Turin in 1982. Since 1983, she has been teacher in several primary schools in the Turin area. From 2015 to 2016, she coordinated the project named "Growing up with media" for the primary school "A. Dasso" of Chivasso. Since 2001, she is responsible of many projects involving multimedia educational activities.

Ruggero G. Pensa received the M.Sc. degree in Computer Engineering from the Polytechnic University of Turin in 2003 and the Ph.D. in Computer Science from INSA of Lyon in 2006. He was adjunct professor at the University of Saint-Etienne (2006-2007); postdoctoral fellow at ISTI-CNR, Pisa (2007-2009); research associate at the University of Turin (2009-2010) and at IRPI-CNR, Turin (2010-2011). Since 2011, he is Assistant Professor at the Department of Computer Science, University of Turin. His main research interests include machine learning, data science, privacy-preserving algorithms for data management, social network analysis and spatio-temporal data analysis. He is member of the editorial board of the Data Mining and Knowledge Discovery journal.