Playing for Privacy Awareness: Learning from a "Wow-Moment" with iBuddy

Felipe Cardoso[1], Davide Andreoletti[1], Alessandro Ferrari[1], Luca Botturi[2], Tiffany Fioroni[2], Chiara Beretta[2], Anna Picco-Schwendener[3], Suzanna Marazza[3] and Silvia Giordano[1]
[1]DTI, Scuola universitaria professionale della Svizzera italiana, Lugano, Switzerland
[2]DFA, Scuola universitaria professionale della Svizzera italiana, Locarno, Switzerland
[3]Competence Centre Digital Law, Università della Svizzera italiana, Lugano, Switzerland
felipe.cardoso@supsi.ch
davide.andreoletti@supsi.ch
alessandro.ferrari@supsi.ch
luca.botturi@supsi.ch
tiffany.fioroni@supsi.ch
chiara.beretta@supsi.ch
anna.picco.schwendener@usi.ch
suzanna.marazza@usi.ch
silvia.giordano@supsi.ch

Abstract: iBuddy is a narrative game-based simulation session inspired by research evidence and designed to enhance secondary school and higher education students' privacy awareness. Students enter the simulation through storytelling and are asked to install the iBuddy app. Later in the simulation, students discover that some of their personal information have been extracted from their devices and manipulated – and this generates a *wow-effect* that sparks questions and discussions. The simulation is backed-up by a lively debriefing phase, supported by original animation videos, interactive activities, and small group games. To overcome privacy issues, iBuddy sessions are played on a local network and the collected data, which are anonymous, are deleted before the end of the session. iBuddy exploits an original software, released as open source, with a layered architecture composed by app, server and operator interface. The system also includes an Artificial Intelligence filter for inappropriate content. Multilingual class materials are published under a Creative Commons license and are available on the www.protectyourdata.ch platform. Post-session assessments collected from over 970 students indicate that they enjoy iBuddy sessions and learn from it. Follow-up assessment data, collected on a portion of the participants, also suggest that iBuddy sessions are effective and conducive to medium-term behavioral change.

Keywords: Privacy education, privacy awareness, simulation, app, secondary education, higher education.

1. Introduction: the challenge of privacy awareness

In the age of digitalization our personal information is continuously exposed on digital devices and networks: privacy concerns each of us. Data privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p.7) Privacy is related with freedom and justice (Kimmel, 1988) and it is a central issue in the progressive digitalization of our society, balancing the power of the Big Tech and of platform capitalism (Srnicek, 2017). Formal education systems included privacy in most digital competence frameworks (e.g., Carretero, Vourikari and Punie, 2017; UK Dept. of Education, 2019). Personal data management, identity management and data protection are, under different names, constituents of active digital citizenship (Carretero, Vourikari and Punie, 2017; JISC, 2014; Guitert, Romeu and Baztan, 2017).

Privacy education initiatives strive to make young people aware of the technical and financial processes that involve our personal data, of our digital traces and profiles (Andreoletti et al., 2020; Eke, Norman, Shuib and Nweke, 2019), and of their value as the "new oil" (Humby, 2006; Giordano et al., 2020). Nonetheless, scholars have identified the so-called *privacy paradox*: although users are generically worried about privacy, many tend to accept disclosure of personal data in exchange of services or popularity (Norberg et al.,2007; Kokolakis, 2017; Barnes, 2006).

In this paper we present the design, development, delivery and assessment of iBuddy, a 2-hour interactive class simulation-based session developed to let young people wonder about personal data capture and storage and to stimulate privacy learning and awareness raising.

2. State of the art

2.1 What we know about privacy awareness

Research evidence supports the claim that most internet users do not consider privacy risks in their behavior, as they are not really aware of them (Ferrari, Puccinelli and Giordano, 2015; Zyfallari, 2021; Andreoletti et al., 2020). Users grant access to personal and sensitive information even to apps that capture considerably more data than actually needed for the services they provide (Vidas, Christin and Cranor, 2011; Felt et al., 2011; Agarwal and Hall, 2013). In many cases, users lack the knowledge and skills to manage their privacy settings (Aditya et al., 2014; Park and Jang, 2015), are seldom aware of relevant regulations and of the economic value of their data (Acquisti, Taylor and Wagman, 2016). However, when they are properly informed, many act consequently (Zyfallari, 2021). For example, in a recent study about 80% of the respondents modified the privacy settings of their social media accounts or reduced their social media usage to feel safer (DuckDuckGo, 2019).

The privacy awareness landscape is heterogeneous. In 2019 a survey with over 20'000 participants from 21 countries reported that in some countries including India, France and the UK, over 50% of the population demonstrated privacy awareness, while several other countries, including the USA and China, seem to lag behind (Statista, 2019).

2.2 Disclosure, rewards, sensitivity and visibility

Despite the evidence of a general increase in privacy awareness, it has been observed that Internet users still tend to accept the disclosure of personal data in exchange for some rewards, without actually wondering how the data will be used and to what purposes. It is interesting to notice that data have economic value for the platforms that collect them, while the nature of user rewards is mostly symbolic (e.g., popularity on social media), thus generating a peculiar asymmetry. We translated these insights into iBuddy's instructional approach: providing participants with an opportunity to experience first-hand the effects of the exposure and capture of personal information that they considered safe. iBuddy aims to generating surprise or, as we labelled it, a *wow-effect* (Kamstrupp, 2016) that facilitates learning.

Pursuing the *wow-effect* required identifying specific situations that would be perceived as risky. A measure of privacy risks can be obtained by combining two main factors (Aghasian et al., 2017): (a) sensitivity, i.e., a measure of how confidential data are; and (b) visibility, i.e., the perceived ease of access to the data. In our work, we considered these two features to develop the simulation. In particular, the iBuddy session stirs students with highly sensitive and apparently difficult to extract data such as pictures from their smartphones.

3. iBuddy

The Making A Privacy Aware World (MAPAW) project, funded under the Agorà Program of the Swiss National Research Foundation, aims to promote personal data protection awareness in young people between 16 and 20 years old. iBuddy was designed and developed as a major action of the MAPAW project.

Thanks to an additional funding by the Swiss national platform Jugend und Medien, some of MAPAW's instruments were adapted and delivered also in lower secondary schools (age group 12-15).

3.1 Instructional principles

The instructional design of iBuddy relies on two assumptions that summarize the discussion above:

1. Deep awareness should be based on factual knowledge (Botturi, 2004): before complying with a list of "do's and don't's", young people need to understand how technologies work and learn to make informed decisions.
2. Generic justice and freedom issues are important, but young people will perceive the relevance of data protection only in relation to personal situations in which sensitivity and visibility are at stake.

At the outset of the project, a design dilemma was identified: research evidence indicates that, in order to make privacy issues relevant, the students' personal experiences and data should be addressed; at the same time, we knew from experience that it is difficult to discuss in class possibly delicate personal situations.

The solution was to transport the activity with the magic circle of a game, more specifically a narrative-based simulation (Betrus and Botturi, 2010), which creates a safe learning environment (Rudolph, Raemer and Simon,

2014; Botturi and Loh, 2009). The personal data of the participants in an iBuddy session become part of a game in which the main character is somebody else – namely a fictional AI-enhanced android classmate.

Game-based learning materials are not new in privacy education, as both class games (Mediasmarts, n.d.; ATED, n.d.) and online games (JRC, n.d.; TSR, n.d.; CISA, n.d.). Such games simulate security threats, but do not directly involve the players and their devices or data: they rely on *understanding* security issues, not on directly experiencing it. A few online games involve players' data and devices: the award-winning *Take this lollipop* (https://takethislollipop.com/) and the more recent *ClickClickClick* (http://clilckclickclick.click). While both share the active engagement-approach, they only work on computers (not on mobile) and are not connected with lesson plans or other instructional materials.

3.2 iBuddy session design

iBuddy sessions are led by a *presenter*, who stands in front of the class and interacts with the students. S/he is supported by an *operator*, who sits at back of the room and manages the iBuddy system. A typical session takes 2 class periods (about 90 min.) and is articulated in the following 6 phases.

Phase 0 | Introduction. The presenter welcomes the students with a predefined narrative, as represented in Figure 1. Students are invited to download and install the iBuddy app, which is a regular Android and iOS app. If some students do not have a smartphone or do not have the permission to install new apps, they can still participate working in pair with a classmate.

> Welcome, my name is [name]!
>
> Before we start, I need you to agree to keep secret what you will experience in the next two hours. In fact, your class has been selected among many for a cutting-edge technological experiment.
>
> In a few weeks, you will welcome a new classmate – but he (or she!) will be special. Indeed, s/he will be a synthetic buddy, made of advanced carbon biotechnical body animated by sophisticated artificial intelligence algorithms. This new buddy will blend in and make your class and your school much better.
>
> Our task today is to configure your new synthetic buddy: determine if it is a boy or a girl, his or her tastes, and so on. In order to do this, we will use a special app.

Figure 1: Narrative introduction to the iBuddy session

Phase 1 | Creating a profile. Once everyone is ready with the app, the presenter unlocks the session. The app behaves as a regular app: it prompts the permission screen for accessing the user's contact list and picture gallery. Students can grant or revoke access, as they like; if asked, the presenter only says: "Feel free to do as you usually do in such cases". The app then asks users to fill in their profile, choosing nickname, favorite food and sport, and adding a profile picture. After that, the app shows eight *basic buddies*, i.e., standard androids with basic features like gender, race and one personal characteristic, e.g., "listener", "patient", "creative", etc. To avoid direct resemblance to real people, the basic buddies are represented in cartoon style (Figure 2).

While students fill in their profile, the iBuddy app copies too the iBuddy local server a sample of 6 pictures from each user's gallery, his/her contacts list, and data on installed apps and their usage time. After pictures have been filtered by an AI algorithm (see below), the *operator* can view the collected data.

Figure 2: Screenshot of the basic buddy profiles

Phase 2 | Class questions. In this phase the wow-effect is generated. Once everyone has picked their favorite basic buddy profile, the app informs the participants to pay attention at the presenter: the configuration procedure now requires the whole group to find collective answers to a few questions. The system resorts here to two different types of questions:

1. *Standard questions* are ready-made and generic and include items like "How many girls are in your class?", "How many of you play soccer?", or "How many of you have a pet?".
2. *Custom questions* are created on-the-fly either by the system automatically or by the operator, using the participants' personal data that the system has collected. A sample of custom questions are presented in Figure 3.

Thanks to the system interface, the presenter can sequence standard and custom questions according to the class reactions. The appearance of supposedly private data on the screen generates a powerful wow-effect, and 3 or 4 custom questions are enough to generate a deep and rich discussion in the following phases. Based on experience and feedback, pictures with simple "everyday" portraits, pets or food are safe and generate a powerful wow-effect. On the other hand, landscapes or objects do not seem to produce a suitable reaction. The session is always concluded with one or two standard questions to chill out the class.

Data used	**Sample custom question**
Installed apps	15 of you use Whatsapp. Shall your new buddy also use this app?
Usage data	On average, you use TikTok 30 hours every month. This is about 1houd a day! Will your new buddy also be such an eager tiktocker?
Contact list	Manu has over 215 contacts in her phone. Will your new buddy also be so popular?
Picture gallery	Deb seems to like pets. Will your new buddy also share this passion? 

Figure 3: Sample custom questions.

Phase 3 | Meet the iBuddy. Eventually, the system then generates the iBuddy profile, which is based on the answers provided in phase 1. The iBuddy is presented to the class (with some fancy visual effects), as in Figure 4. The iBuddy is the MacGuffin that sets the whole session in motion and the actual result, although often welcomed with thrill, is not very important for the learning process. The simulation ends here.

Figure 4: Presentation of the customized buddy.

Phase 4 | Debriefing part A: behind the scenes. Simulation-based and game-based learning is triggered by playing but is made solid by debriefing (Betrus and Botturi, 2010; Peters and Vissers, 2004). The debriefing of an iBuddy session happens in two steps. In the "behind the scenes" step the students are led to interrogate the simulation: what "tricks" let the system grab their data to generate custom questions? The presenter explains how the app accessed and transmitted personal data to the local server, and that this is what many apps also do. The system includes a summary interface that shows the key figures of the collected data. Reflections on how such data can be fed into AI algorithms to infer additional digital profile details are also brought in. Eventually, the presenter clicks on "the red button" and deletes all personal data from the iBuddy server.

Phase 5| Debriefing part B: our data on the Internet today. The second debriefing step explores how personal data are collected, stored and elaborated in real life. It focuses on regular and legal uses of personal data (e.g., personalized advertisement) rather than on malicious uses (e.g., identity fraud), and its structure depends on the questions the participants ask. For this part, the presenter is equipped with modular original learning materials, including a set of 4 short digital stop-motion video clips, groupwork activities and a list of useful websites. All original materials are available at www.protectyourdata.ch in Italian, French, German and Rumantsch under a CC License. The platform also provides a database of useful privacy education resources.

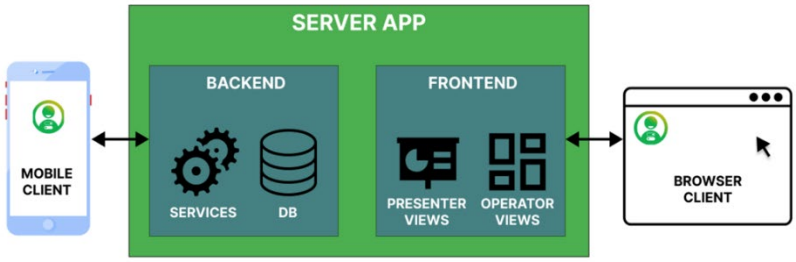
4. Software design and implementation

The iBuddy system is composed by two main software applications (apps): a Server app and a Mobile app. The Server app is a web-based software responsible for the data processing (backend) and that allows presenter and operator to interact with captured user data (frontend). The Mobile app is the software that students interact with, and it is compatible with both iOS and Android smartphones.

4.1 Functional and technical architecture

The technical architecture of iBuddy was devised to provide a smooth, entertaining and technically safe session. The functional architecture is composed by three parts, as in Figure 5:

1. A Mobile app (client) which students interact with, that manages the data collection (contacts, pictures, applications list, applications usage) during the session. The Client features a multi-language interface.
2. A Server App that receives and processes the collected data. The server is composed of two sub-components: (a) the Backend, that manages the collected data, performs statistics, generates questions and filters content; and (b) the Frontend, that allows presenter and operator to access Backend services via web views, i.e., interfaces and data visualizations.
3. A Browser Client to access the Frontend web views.



1.

Figure 5: Representation of the iBuddy functional architecture, composed of mobile app, backend, frontend and browser client.

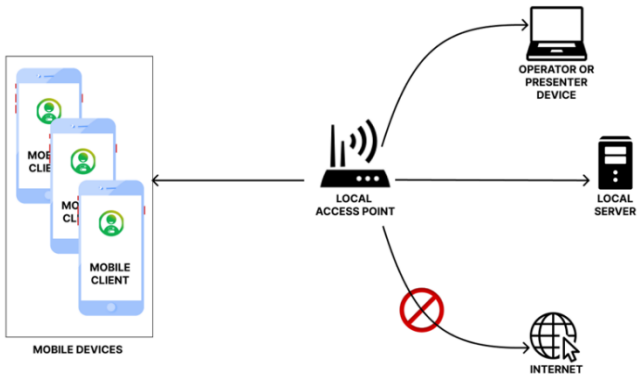


Figure 6: Representation of the physical architecture, composed of a local access point to which students and presenter/operators connect and a local server for data storage and processing.

The physical architecture includes at least the following devices (Figure 6):

1. Mobile devices: students' mobile phone(s), running the iBuddy Mobile app.
2. Operator and Presenter devices: a device through which presenter and operator access the Frontend.
3. Local Server: a desktop or mobile computer where the iBuddy server runs. This can be a separate computer or the computer used by the operator or the presenter.
4. Local Access Point: a device that manages the local network with no internet access. The users' devices and the local server are connected to the local network and disconnected from the Internet to avoid any unauthorized access or leak of the data collected during the session.

4.2 Web views

The Frontend component exposes several web views. The most important ones are the presenter view, that allows the Presenter to lock/unlock the session, to show/hide questions and introduce the final iBuddy; and the Operator view, which allows to create and edit custom questions by using collected pictures from students' devices (Figure 7).

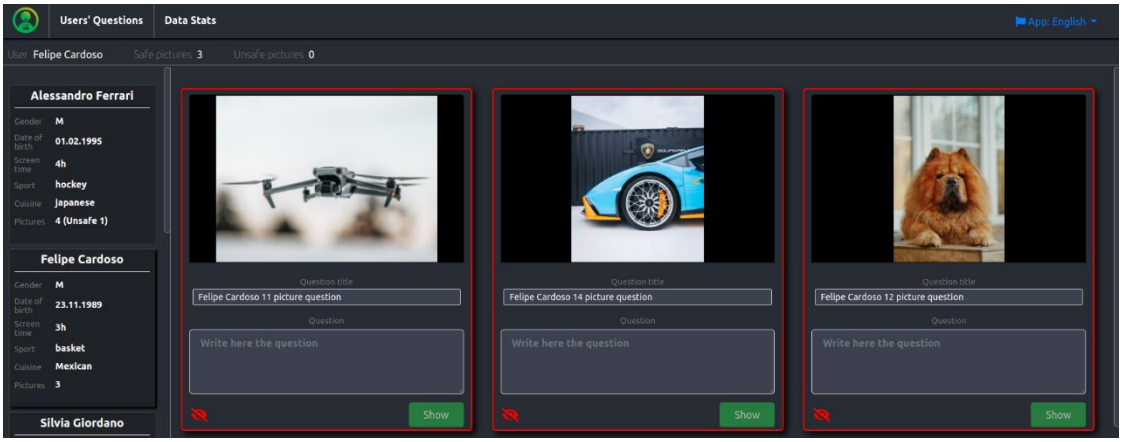


Figure 7: A screenshot of the operator view.

4.3 Services

Besides simple data management, the Backend component provides three additional main services:

1. Statistic. The statistics service extracts insights from the collected data, i.e., contacts, pictures, installed apps and apps usage. The goal of this service is to provide materials for generating custom questions during Phase 2 and to show students an overview of the collected data in Phase 4.
2. Questions generation. The questions generator is a service that periodically computes statistics and automatically creates questions about some interesting figures, like the average number of items in contact lists. Specifically, the service generates custom questions by selecting and filling generic question templates based on the outcomes of the statistics service. Templates are provided in multiple languages.
3. AI Unsafe Content Filter. The content filter is a service that constantly monitors all the pictures collected from the users' devices and checks if any of them contains unsafe content. The service is powered by an

AI-trained model, from NSFW JS library creators1, which classifies images in the following categories: drawings, hentai, sexy, porn and neutral. As it can be observed from the confusion matrix in Figure 8, the model is capable to identify the correct category with a high accuracy (always greater than 91% across all the considered categories). The performance of the model is depicted by the confusion matrix in Figure 8. Only the images classified as "neutral" will be made available to the operator, while the remaining ones are discarded. To reduce the likelihood of false negatives (i.e., images that are wrongly considered neutral by the model), we set a safety threshold on the score associated with the neutral class, selecting only images with neutral score above 0.55 (on a 0-1 range).

5. Legal aspects

Collecting students' data from their smartphones for teaching purposes might seem ethically extreme. Actually, the data collection happens every day with many commercial applications and web services: the whole point with iBuddy is making the process visible by completing it in a short time and inside the classroom. iBuddy was designed to meet the requirements of the Swiss Federal Act on Data Protection[2] and respect ethical standards.

Swiss laws do not set a minimum age for consenting to data processing, which depends on "discernment capacity". As a solution to this issue, we developed a clear and full explanation of the iBuddy system and of the way data are processed throughout the simulation for the school's headmaster and for the teacher in charge, who must be in class during the simulation.

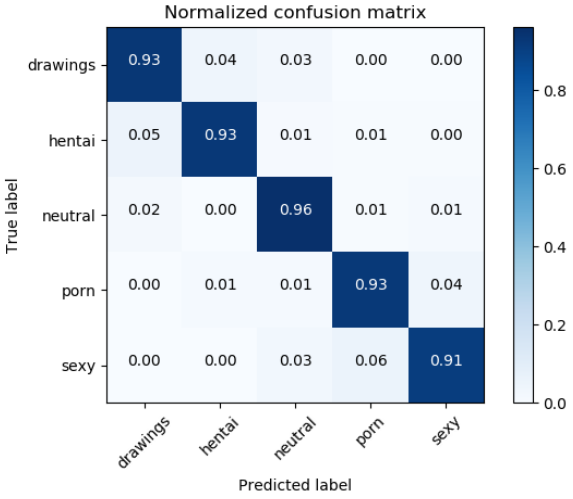


Figure 8: Confusion matrix of the AI-based model trained to detect inappropriate images.

Moreover, each student is free to access the privacy policy properly attached to the iBuddy app, which is available anytime. Students can also grant separate and specific consent for access to the photo folder and the contacts list of her/his phone. Without explicit consent, the operator is not allowed to capture and process any photo and/or contact item, the system not being even able to access them. During the sessions held so far, part of the pupils granted their consent while others denied it with varying proportions in different classes, and the presenter took this as an opportunity to discuss the consequences of granting and denying consent for data processing.

Even if the aim of the simulation is to achieve a wow-effect, we published a proper, easy to understand privacy policy to comply with the law, and part of the debriefing is indeed also about going through it to raise awareness about this important but often neglected text.

When starting the simulation, the app prompts the user to write a nickname. This choice, instead of the actual name, was done so that neither the presenter nor the operator could connect the data to any subject.

[1] https://github.com/infinitered/nsfwjs
[2] Federal Act on Data Protection of 19 June 1992 (RS 235.1)

As mentioned above, data are kept in a single copy on a local server with no Internet connection, so that no interference with unauthorized third parties is possible. Last but not least, all personal data are deleted during the session itself, which usually means about 30 minutes after their collection.

6. Experimentation and lessons learned

Between March 2021 and March 2022, 52 iBuddy sessions were carried out, engaging a total of 978 students in 17 schools, as illustrated in Table 1. Students engaged deeply (even asking if they would actually welcome a synthetic buddy in their class!) and, during the debriefing, asked many questions and mentioned personal experiences. Both students' and teachers' informal feedback was positive, at times enthusiastic.

Table 1: Schools, classes and students by school level

	Secondary school		High school	University	TOTAL
Age range	11-12y	13-14y	15-19y	20+	
Classes/Groups	20	11	17	4	52
Students	344	219	343	72	978
Schools	10		6	1	17

6.1 Post-session feedback

A short post-session survey was used to collect structured feedback. It was composed by 4 closed and 4 open items and was administered during the last 10 minutes of every session. Closed questions were rated on a 1 (lowest)-to-10 (highest) scale, and the evaluation items were:

1. Enjoyment: how much did you enjoy this activity?
2. Usefulness: how useful is this activity in raising awareness among young people about a responsible use of their personal data?
3. Involvement: how involved did you feel in these issues?
4. Importance: how important do you think the topics are?

All participants across all school levels found the topic of data privacy very *important* (M=8.96) and the activity very *useful* (M=8.58) and *enjoyable* (M=7.82), consistently indicating that iBuddy sessions achieved their immediate goal. The breakout of the different school levels (Figure 9) reveals that younger participants have weaker personal involvement. The global average score for *involvement* is overall lower (M=7.09) and increases with the age of the participants. A possible explanation is that high school students more often own personal devices and have at the same time more sophisticated behaviors and less parental guidance.

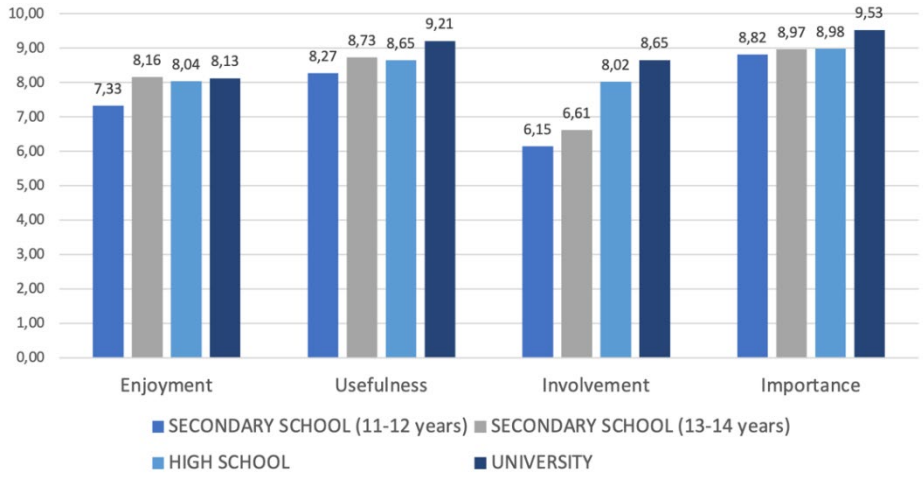


Figure 9: Average scores obtained in the various categories (N=978)

The answers to the open questions suggest that students appreciated the simulation. This very interactive part aroused interest and some participants felt personally touched when their personal data (especially photographs) appeared on the screen in front of everyone. Many students claimed to have been surprised by the ease and speed with which their personal data were captured and appreciated the fact that iBuddy reproduced a similar experience to what happens in real life with apps and social networks. After an initial moment of disorientation, the students quickly realized that their data were not being "hacked", but rather that

they had actively granted access when they had accepted (without reading!) the terms of use of the iBuddy application. Such element of awareness is of course crucial to promote privacy awareness.

Moreover, many participants realized for the first time the economic value of their personal data, which is often underestimated, and were amazed to find out what really goes on behind the scenes of their mobile phones. In the debriefing, the students appreciated the animated video clips, the activities carried out in groups and the discussions established with the presenter.

6.2 Follow-up assessment

Positive post-session feedback not necessarily corresponds to actual long-term learning. Two months after each session, the secondary school participants received an invitation to fill in a short follow-up survey. 563 participants were contacted, and 22% responded (N=124, 57 males and 67 females). The follow-up survey included 7 items starting with "After the iBuddy session…", for which respondents indicated the level of agreement on a 3-point Likert scale, ranging from "like before" (value 0) to "much more than before" (value 2):

1. … I pay attention when I install a new app
2. … I read or at least screen the terms of use of the apps I install
3. … I check and adjust privacy setting for my social network accounts
4. … I select what I post or share on social networks
5. … I think about why some ads appear when I browse the web
6. … I check and maybe delete cookies on my devices
7. … I am generally aware about my personal data

While the general item "I am more aware about personal data" received the highest impact score (1.15), lower scores were measured for more specific items (Figure 10). This corresponds to previous findings and to the privacy paradox idea. In general, participants seem to pay more attention to frequent active behaviors (e.g., adjusting privacy settings; selecting content to post; etc.), and less to rare passive ones (e.g., managing cookies; reading terms of use; etc.). Adding up all the seven scores, it is possible to calculate a unique indicator ranging from 0 to 14. Interestingly, only 20 participants (16%) have a high score (>9) and 14 are girls.

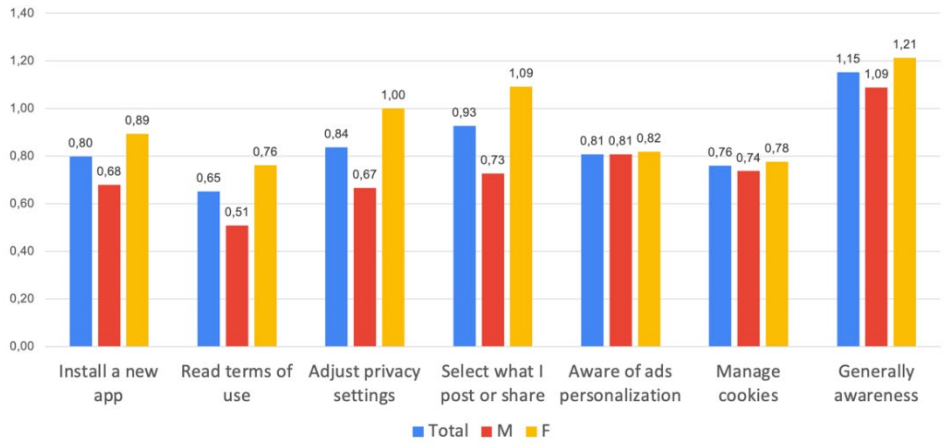


Figure 10: Follow-up survey data (N=124)

7. Discussion and conclusions

This paper presented iBuddy, a narrative simulation that promotes privacy awareness in secondary and higher education students. The iBuddy system and the 2-hour session in which it is used were designed based on research evidence in privacy awareness, and its positive post-session and follow-up assessment results confirm the effectiveness of its approach.

iBuddy is an ongoing project. On one hand, we are currently working to make the system and its related teaching and learning materials easily accessible in multiple languages. This includes both making the iBuddy system downloadable and providing it on light-weight hardware (e.g., Raspberry). On the other, we are fine-tuning the session design in two directions: (a) developing different narratives, that might be more appealing and engaging for different target groups; (b) designing a "closed" session in which students do not use their personal devices.

This latter situation can better meet the regulations of individual schools or school systems, and clears all potential legal issues connected with accessing student data during the simulation.

Overall, the iBuddy experience provides evidence that a game-based approach can be effective to tackle complex and potentially delicate learning topics, such as privacy and personal data protection, promoting engagement and medium-term behavioural changes.

References

Acquisti, A., Taylor, C. R., and Wagman L. (2016) "The economics of privacy", *Journal of Economic Literature,* Vol 52, No. 2, pp 442-492.

Aditya, P., Bhattacharjee, B., Druschel, P., Erdèlyi, V. and Lentz, M. (2014) "Brave New World: Privacy Risks for Mobile Users", *SPME'14 Proceedings of the ACM MobiCom workshop on Security and privacy in mobile environments*, pp 7-12.

Agarwal Y, and Hall, M. (2013) "ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing", *Proceedings of the 11th annual international conference on Mobile systems, applications, and services, ACM*, pp 97-110.

Aghasian, E., Garg, S., Gao, L., Yu, S., and Montgomery, J. (2017) "Scoring users' privacy disclosure across multiple online social networks", *IEEE access*, Vol 5, pp 13118-13130. doi:10.1109/access.2017.2720187.

Andreoletti, D., Luceri, L., Braun, T., Tornatore, M., and Giordano, S. (2020) "Measurement and Control of Geo-Location Privacy on Twitter", *Online Social Networks and Media,* Vol 17, 100078.

ATED (n.d) *Cyber Survival Game*. https://www.cybersurvivalgame.ch/

Barnes, S. B. (2006) "A privacy paradox: Social networking in the United States", *First Monday*, Vol 11, No. 9.

Betrus, A., and Botturi, L. (2010) "Principles of using simulations and games for teaching". In A. Hirumi (ed.), *Playing Games in Schools: Engaging Learners through Interactive Entertainment*, International Society for Technology in Education, pp 33–55.

Botturi, L. (2004) "Visualizing Learning Goals with the Quail Model", *Australasian Journal of Educational Technologies*, Vol 20, No. 2, pp 248-273. https://doi.org/10.14742/ajet.1362

Botturi, L., and Loh, C. S. (2009) Once Upon a Game: Rediscovering the Roots of Games in Education. In C. T. Miller (ed.), *Games: purpose and potential in education*, New York: Springer, pp 1-22.

Carretero, S., Vourikari, R., and Punie, Y. (2017) *DigComp 2.1. The Digital Competence Framework for Citizens.* Luxembourg: Publications Office of the European Union, 2017.

CISA (n.d.) Cybersecurity games https://www.cisa.gov/cybergames

DuckDuckGo privacy research. (2019) *New DuckDuckGo Research Shows People Taking Action on Privacy*. https://spreadprivacy.com/people-taking-action-on-privacy/

Eke, C. I., Norman, A. A., Shuib, L., and Nweke, H. F. (2019) "A survey of user profiling: State-of-the-art, challenges, and solutions", *IEEE Access*, Vol 7, pp 144907-144924.

Felt, A. P., Chin, E., Hanna, S., Song, D., and Wagner, D. (2011) "Android permissions demystified", *Proceedings of the 18th ACM conference on Computer and communications security 2011*, pp 627-638.

Ferrari, A., Puccinelli, D., and Giordano, S. (2015) "Managing your privacy in mobile applications with mockingbird", presented at *PERCOM Workshops*.

Giordano, S., Morel, V., Önen, M., Musolesi, M., Andreoletti, D., Cardoso, F., Ferrari, A., Luceri, L., Castelluccia, C., le Métayer, D., Van Rompay, C., and Baron, B. (2020) "UPRISE-IoT: User-Centric Privacy and Security in the IoT". In J. Hernandez-Ramos and A. Skarmeta (ed.), *Security and Privacy in the Internet of Things: Challenges and Solutions,* IOS Press, pp 44-60.

Guitert, M., Romeu, T., and Baztan, P. (2017) "Conceptual framework on digital competences in primary and secondary schools in Europe", *Proceedings of ICERI 2017*, pp 5081-5090.

Humby, C. (2006) "Data is the new oil", *Proceedings og ANA Sr. Marketer's Summit*. Evanston, IL, USA.

JISC (2014) *Developing digital literacies*. https://www.jisc.ac.uk/guides/developing-digital-literacies

JRC (n.d.) *Cyberchronix*. https://visitors-centre.jrc.ec.europa.eu/cyber-chronix/

Kamstrupp, A. K. (2016) "The wow-effect in science teacher education", *Cultural Studies of Science Education*, Vol 11, No. 4, pp 879-897.

Kimmel, A. (1988) *Ethics and values in social research*. London: Sage.

Kokolakis, S. (2017) "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon", *Computers and Security,* Vol 64, pp 122-134, doi:10.1016/j.cose.2015.07.002

Mediasmarts (n.d.) *Privacy Pirates Cyber Survival Game*. https://mediasmarts.ca/game/privacy-pirates-interactive-unit-online-privacy-ages-7-9

Norberg, P. A., Horne, D. R. and Horne, D. A. (2007) "The privacy paradox: Personal information disclosure intentions versus behaviors", *Journal of consumer affairs*, Vol 41, No. 1, pp 100-126.

Park, Y. J., and Jang, S M. (2014) "Understanding Privacy Knowledge and Skill in Mobile Communication", *Computer Human Behaviour,* Vol 38, pp 296-303.

Peters, V. A., and Vissers, G. A. (2004) "A simple classification model for debriefing simulation games", *Simulation & Gaming*, Vol 35, No. 1, pp 70-84.

Rudolph, J. W., Raemer, D. B., and Simon, R. (2014) "Establishing a safe container for learning in simulation: the role of the presimulation briefing", *Simulation in Healthcare*, Vol 9, No. 6, pp 339-349.
Srnicek, N. (2017) *Platform capitalism*. John Wiley and Sons.
Statista (2019) *Share of internet users worldwide who are aware of their country's data protection and privacy rules*. https://www.statista.com/statistics/1015277/data-protection-and-privacy-rule-awareness-by-country/
TSR (n.d.) *DataK*. https://datak.rts.ch/ecoles/
UK Dept. of Education (2019). *Essential digital skills framework*.
Vidas, T., Christin, N., and Cranor, L. (2011) "Curbing android permission creep", *Proceedings of the Web*, Vol 2, pp 1-5.
Westin, A. F. (1967) "Special report: legal safeguards to insure privacy in a computer society", *Communications of the ACM*, Vol 10, No. 9, pp 533-537.
Zyfallari, V. (2021) *Are people aware of their data value? An experimental study of users' privacy perception when using mobile phone apps.* SUPSI Master Thesis.